Maisterintutkielma

Tietojenkäsittelytiede

Privacy by Design: EU:n yleisen tietosuoja-asetuksen vaikutukset sovelluskehitykseen

Nina Bärlund-Vihtola

3.5.2020

Matemaattis-luonnontieteellinen tiedekunta

Helsingin yliopisto

Ohjaaja(t)

Prof. Tomi Männistö

Tarkastaja(t)

Yhteystiedot

PL 68 (Pietari Kalmin katu 5)
00014 Helsingin yliopisto

Sähkopostiosoite: info@cs.helsinki.fi
URL: http://www.cs.helsinki.fi/

HELSINGIN YLIOPISTO – HELSINGFORS UNIVERSITET – UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Koulutusohjelma — Utbildningsprogram — Study programme
Matemaattis-luonnontieteellinen tiedekunta	Tietojenkäsittelytiede

Tekijä — Författare — Author

Nina Bärlund-Vihtola

Työn nimi — Arbetets titel — Title

Privacy by Design: EU:n yleisen tietosuoja-asetuksen vaikutukset sovelluskehitykseen

Ohjaajat — Handledare — Supervisors

Prof. Tomi Männistö

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Maisterintutkielma	3.5.2020	105 sivua, 24 liitesivua

Tiivistelmä — Referat — Abstract

Henkilötietojen suoja eli tietosuoja on Euroopan unionin perusoikeuskirjassa vahvistettu perusoikeus. Yksityishenkilöiden tietosuoja vahvistui entisestään, kun vuonna 2018 alettiin kaikissa EU:n jäsenmaissa soveltaa Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, lyhyemmin EU:n yleistä tietosuoja-asetusta. Asetusta täydennettiin myöhemmin kansallisella tietosuojalailla 1050/2018.

Organisaatio, joka omistaa henkilörekisterin, on rekisterinpitäjä, ja henkilö, jonka tiedot ovat henkilörekisterissä, rekisteröity. Tietosuoja-asetuksessa on määritetty rekisterinpitäjän velvollisuudet, joiden avulla tämän on vastattava siitä, että rekisteröidyn oikeudet toteutuvat. Lisäksi rekisterinpitäjällä on osoitusvelvollisuus siitä, että henkilötietojen käsittely tapahtuu tietosuoja-asetuksen käsittelyperiaatteiden mukaisesti, sekä ilmoitusvelvollisuus kansalliselle valvontaviranomaiselle tilanteissa, joissa on tapahtunut henkilötietojen tietoturvaloukkaus.

Tietosuoja-asetuksella on vaikutuksia sovelluskehitykseen. Asetus velvoittaa huolehtimaan sisäänrakennetusta tietosuojasta (Privacy by Design) eli tietosuojaa tuottavien toiminnallisuuksien toteutuksesta tietojärjestelmiin alusta alkaen. Asetus on pitkä ja hankala, joten ollut organisaatioille työlästä havaita siitä kaikki velvoitteet. Tässä tutkielmassa on pyritty vastaamaan tuohon ongelmaan etsimällä asetuksesta sisäänrakennetun tietosuojan vaatimukset ja kiinnittämällä ne TOGAF-kokonaisarkkitehtuurikehykseen. Tämän pohjalta on toteutettu sovelluskehityksen tietosuojaohjeistuksen runko, jota kehittämällä on organisaatiolle luotavissa toimiva ohjeistus sisäänrakennetun tietosuojan rakentamisen tueksi.

ACM Computing Classification System (CCS)
Security and privacy → Human and societal aspects of security and privacy → Privacy protections
Software and its engineering → Designing software → Software design engineering
Software and its engineering → Designing software → Requirements analysis

Avainsanat — Nyckelord — Keywords

tietosuoja-asetus, sisäänrakennettu tietosuoja, sovelluskehitys, kokonaisarkkitehtuuri

Säilytyspaikka — Förvaringsställe — Where deposited

Helsingin yliopiston kirjasto

Muita tietoja — övriga uppgifter — Additional information

Ohjelmistojärjestelmien erikoistumislinja

Sisältö

1 Johdanto

Teknologian kehittyminen, digitalisaatio ja globalisaatio ovat lisänneet henkilötietojen keräämisen helppoutta, nopeutta ja laajuutta: henkilötiedot liikkuvat verkossa nopeasti ja näkymättömästi ilman, että henkilöllä itsellään on siihen välttämättä mahdollisuutta vaikuttaa. Tämä on myös mahdollistanut henkilötietojen käyttämisen entistä helpommin myös haitallisiin tarkoituksiin.

Kun toimimme digitaalisessa ympäristössä, jää liikkumisestamme verkossa ja toimistamme eri palveluissa merkintöjä, jotka kertovat tekemisistämme ja joista meidät on mahdollista tunnistaa. Saatamme itsekin antaa itsestämme tietoja eri palveluihin sen enempää ajattelematta, minne tiedot kertyvät ja mitä niillä jatkossa tullaan tekemään. Kun asioimme sähköisesti tai muilla tavoin eri organisaatioiden kanssa, keräävät ne meistä informaatiota asiointiin liittyen. Jos kerättyjen tietojen perusteella on mahdollista joko suoraan tai tietoja toisiinsa yhdistellen selvittää, keneen fyysiseen henkilöön ne liittyvät, silloin tiedot ovat tietosuojan alaisia henkilötietoja. Jos tiedot on tallennettu tietojoukoksi, josta tiedot on tarvittaessa haettavissa esille ja liitettävissä tiettyyn fyysiseen henkilöön, on kyseessä henkilörekisteri. EU:n yleinen tietosuoja-asetus [7] pyrkii turvaamaan yksityisyyttämme näiden henkilörekistereihin tallennettujen henkilötietojemme osalta antamalle meille rekisteröidyille erikseen määriteltyjä oikeuksia omiin tietoihimme ja niihin liittyviin toimenpiteisiin.

Henkilötietojen suoja eli tietosuoja on Euroopan unionin perusoikeuskirjassa 2016/C202/02 [9] vahvistettu itsenäinen perusoikeus. Henkilötietojen suoja on myös osa yksityiselämän suojaa, josta säädetään Suomen perustuslaissa 731/1999 [27]. Vahvistusta yksityishenkilöiden tietosuojasta säädettyihin lakeihin tuli vuonna 2016, jolloin astui voimaan Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta [7], lyhyemmin EU:n yleinen tietosuoja-asetus (myöhemmin tietosuoja-asetus), jota ryhdyttiin koko EU:n alueella soveltamaan toukokuussa 2018. Tietosuoja-asetukseen viitataan usein myös lyhenteellä GDPR, joka tulee sen englanninkielisestä nimestä General Data Protection Regulation. EU:n asetukset ovat suoraan EU:n jäsenvaltioissa sovellettavaa oikeutta, jota on mahdollista täsmentää ja täydentää kansallisilla laeilla niissä puitteissa kuin asetukseen on

kansallisesta säätelyvarasta kirjattu. Suomessa tietosuoja-asetusta täydennettiin tietosuojalailla 1050/2018 [29], joka astui voimaan vuoden 2019 alusta. EU-asetuksella ja kansallisella lailla kumottiin aiemmin henkilötiedon käsitettä ja henkilötietojen käsittelyä säännelleet EU:n henkilötietodirektiivi 95/46 [8] ja sen Suomessa täytäntöön pannut henkilötietolaki 523/1999 [12]. Tietosuoja-asetus ja tietosuojalaki yhdessä määrittelevät henkilötietojen käsittelyn periaatteet Suomessa. Näiden lakien lisäksi Suomessa on olemassa huomattava määrä erityislakeja, joilla säädellään henkilötietojen käsittelyä määrätyissä tilanteissa.

Tietosuoja on jokaisen luonnollisen henkilön perusoikeus, jonka avulla pyritään turvaamaan hänen oikeuksiensa toteutuminen hänen henkilötietojensa käsittelyn yhteydessä. Tietosuoja-asetuksen [7] tarkoituksena on lisätä henkilötietojen rekisteröinnin ja käsittelyn läpinäkyvyyttä ja avoimuutta asettamalla palveluita tuottaville organisaatioille lainsäädännön avulla vaatimuksia, jotka näiden on palveluita toteuttaessaan ja tuottaessaan otettava huomioon. Asetuksen tavoitteena on myös yhdenmukaistaa henkilötietojen käsittely EU:n alueella ja turvata henkilötietojen liikkuvuus EU:n jäsenmaiden välillä. Teknologian kehittyminen ja globalisaatio ovat tuoneen uusia haasteita henkilötietojen suojelemiseen. EU pyrkii tietosuoja-asetuksen avulla suojaamaan kansalaistensa henkilötietoja asuinmaasta ja kansallisuudesta riippumatta niin, että rekisteröidyllä henkilöllä on mahdollisuus itse vaikuttaa omien henkilötietojensa käsittelyyn aiempaa paremmin. Vastuu henkilötietojen käsittelystä asetuksen hengen mukaisesti on organisaatioilla, jotka henkilötietoja keräävät. Niille on tietosuoja-asetuksessa määritetty runsaasti vaatimuksia siitä, miten henkilötietojen käsittelyä tulisi ohjata, toteuttaa ja valvoa niin, että rekisteröityjen henkilöiden oikeudet toteutuvat. Merkittävin uudistus verrattuna aiempaan henkilötietolakiin on organisaatioille asetettu osoitusvelvollisuus, jonka mukaan organisaatiolla on oltava kyvykkyys kysyttäessä näyttää toteen, että se on hoitanut henkilötietojen käsittelyä tietosuoja-asetuksen velvoitteiden mukaisesti.

Nykypäivän digitaalisessa maailmassa, jossa tieto liikkuu sähköisessä muodossa eri tietojärjestelmien ja sovelluspalveluiden välillä omistajansa näkymättömissä, on tietojärjestelmiä kehittävillä ja ylläpitävillä asiantuntijoilla suuri vastuu tietosuojan toteutuksesta kaikissa organisaatioissa. Rekisteröityjen henkilöiden oikeuksien toteutuminen organisaation toiminnassa vaatii sovelluskehitystä tekeviltä asiantuntijoilta ymmärrystä EU:n tietosuoja-asetuksen ja kansallisen tietosuojalain sisällöstä sekä käsitystä sellaisista sovellusarkkitehtuuriin liittyvistä päätöksistä, toimenpiteistä ja teknisistä ratkaisuista, joiden avulla on mahdollista pyrkiä vaadittuun lopputulokseen ja osoitusvelvol-

lisuuden täyttämiseen. Tietosuoja-asetuksessa yhdeksi organisaation velvoitteeksi on asetettu sisäänrakennetun tietosuojan toteutuminen. Asetuksessa ei kuitenkaan erityisen selvästi määritellä, mitä termi tarkoittaa. Tässä tutkielmassa on selvitetty, minkälaisia vaatimuksia tietosuojan toteuttaminen asettaa organisaation sovelluskehitykselle ja miten sisäänrakennettu tietosuoja implementoidaan organisaation tietojärjestelmiin. Näiden tehtyjen havaintojen pohjalta toteutettiin ensimmäinen versio sovelluskehityksen tietosuojaohjeistuksesta Maanmittauslaitoksen sovelluskehittäjiä varten.

1.1 Tutkimuskysymykset

Tutkielmassa on tarkasteltu toukokuussa 2018 sovellettavaksi tullutta EU:n yleistä tietosuoja-asetusta [7] sovelluskehityksen näkökulmasta. Pyrkimyksenä on ollut löytää tietosuoja-asetuksesta ja muusta henkilötietojen käsittelyyn vaikuttavasta kansallisesta lainsäädännöstä ne organisaatioille asetetut tietosuojavaatimukset, joiden täyttämiseen on mahdollista vaikuttaa sovelluskehityksessä joko arkkitehtuurin ja sovelluksen toiminnallisuuksien tai niiden dokumentoinnin avulla. Johtoajatuksena on sisäänrakennetun tietosuojan (Privacy by Design) periaate, jonka vaikutusta sovellusarkkitehtuuriin ja sovelluskehitykseen on tutkielmassa käsitelty.

Tutkielmassa on keskitytty seuraaviin tutkimuskysymyksiin:

> TK1 Minkälaisia vaatimuksia EU:n yleinen tietosuoja-asetus asettaa sovelluskehitykselle?
>
> TK2 Minkälaista ohjeistusta sovelluskehittäjät tarvitsevat sisäänrakennetun tietosuojan huomioimiseksi sovelluskehityksessä?

Sovelluskehitystä varten on olemassa useita erilaisia systeemityömenetelmiä ja -malleja, joita voidaan käyttää tietojärjestelmien kehittämisen varsinaisessa sovelluskehitysosuudessa. Tutkielmassa ei kuitenkaan ole perehdytty näihin malleihin. Sen sijaan, jotta tietosuoja-asetuksen vaatimukset sovelluskehitykselle osattaisiin ottaa huomioon riittävän ajoissa eli jo silloin, kun kehittämishanketta vasta suunnitellaan, on tutkielmassa haluttu kiinnittää sovelluskehitykseen vaikuttavat tietosuojavaatimukset kokonaisarkkitehtuurin kehittämiseen. Tutkielmassa käytettäväksi arkkitehtuurin kehittämismalliksi valittiin laajalti käytetty kokonaisarkkitehtuurikehys TOGAF [24], jonka kuvaaman arkkitehtuurin kehitysprosessin (Architecture Design Model, ADM) vaiheisiin vaatimukset on tutkielmassa kiinnitetty.

Tutkielmassa tarkasteltiin tietosuoja-asetuksen vaatimuksia, jotka liittyvät organisaation jokapäiväiseen operatiiviseen henkilötietojen käsittelyyn. Asetuksessa ja muissa laeissa kuvatut poikkeukset henkilötietojen käsittelyyn ja esimerkiksi henkilötietojen julkisuuteen todetaan, mutta niiden tarkempi käsittely on rajattu pois tutkielmasta. Näitä poikkeuksia ovat muun muassa sananvapauden ja tiedonvälityksen vapauden turvaamiseen sekä journalistiseen, akateemiseen, taiteelliseen tai kirjalliseen ilmaisuun liittyvät erivapaudet, sekä tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tai yleisen edun mukaisia arkistointitarkoituksia varten tehtävä henkilötietojen käsittely. Samoin tietosuoja-asetuksen sisällöstä on esitelty vain ne kohdat, jotka koskevat yksittäisen organisaation tietosuojatyötä. EU-tasoiset vastuut, yhteistyö jäsenvaltioiden ja niiden tietosuojatoimijoiden välillä sekä EU-tasoisten lainsäädäntöorgaanien toiminta on rajattu tutkielmasta pois epärelevanttina sen aiheelle.

1.2 Tutkimusmenetelmät

Tutkielma tehtiin tapaustutkimuksena [5] rajautumalla tietyn tämän päivän ilmiön eli henkilötietojen tietosuojan tutkimiseen tietyn lähteen eli lakitekstien kautta. Tutkielman tavoitteena oli kehittää tutkimuskohteena olevan organisaation toimintaa. Tutkija toteutti tutkimuksen kyseisen organisaation luvalla ja toimeksiannosta osallistuen aktiivisesti organisaatiossa henkilötietojen tietosuoja soveltamista liittyvään toimintaan. Tutkielman lopputuotoksena syntynyt ohjeisto tuottaa organisaatiolle lisäarvoa aiempaa havainnollisempana toimintamallina, jonka avulla toiminnan parantaminen tutkimusaiheen sektorilla on mahdollista.

Tutkielma toteutettiin alkuvuoden 2020 aikana. Tutkimuksen vaiheistus oli seuraava:

- Taustaselvitys ja tietosuoja-asetuksen vaatimusten keräily
- Vaatimusten analysointi ja arviointi arkkitehtuurikehyksen näkökulmasta
- Haastattelututkimusosuus ja artefaktin toteuttaminen
- Tutkielman viimeistely ja palauttaminen

Tutkielman aloittaa taustoittava katsaus tutkimuksen kohteena olevista laeista ja asetuksista. Katsauksessa kyseiset lait on esitelty ja niistä on nostettu esiin lainkohdat, jotka vastaavat ensimmäiseen tutkimuskysymykseen. Vastauksena tutkimuskysymykseen havaitut

DSRM-vaihe	Tutkimuksen toteutus
Tutkimusongelman identifiointi	Maanmittauslaitoksen sovelluskehityksen tarvitsema ohjeistus sisäänrakennetun tietosuojan implementoimiseksi tietojärjestelmiin sekä rekisterinpitäjälle asetetun osoitusvelvollisuuden täyttämiseksi sovellusarkkitehtuurin osalta
Ratkaisun tavoitteiden määrittely	Haastattelututkimus 19 Maanmittauslaitoksen asiantuntijalle, joista - 11 sovelluskehityksen asiantuntijaa - 8 teknologiaympäristön, lokituksen tai kokonaisarkkitehtuurin asiantuntijaa Haastattelujen tavoitteena tietosuojaohjeistuksen rakenteeseen ja sisältöön liittyvien tarpeiden ja toiveiden kerääminen
Ratkaisun suunnittelu ja toteutus	Haastatteluyhteenvedon tekeminen ja toiveiden ryhmittely rakenteellisiin ja sisällöllisiin toiveisiin Rakenteellisten toiveiden toteuttaminen eli ohjesivuston sivutyyppien määrittely ja niiden välisten yhteyksien hahmottelu Tutkimuksen tulosten eli tietosuoja-asetuksen periaatteiden ja vaatimusluettelon sijoittaminen sivustolle Valittujen sisällöllisten toiveiden toteuttaminen eli tarvittavien toimenpiteiden (muistilistojen) kirjaaminen sivuille
Ratkaisun esittely tai havainnollistaminen	Ratkaisun esittäminen neljälle tietosuojaan perehtyneelle asiantuntijalle Ratkaisun selostaminen kirjallisesti (sisältäen hyperlinkin sivustoon) 33 Maanmittauslaitoksen asiantuntijalle ja kuudelle esimiehelle
Ratkaisun käytettävyyden arviointi	Asiantuntijoiden tutustuminen ohjesivustoon ja kommentointi tutkimuksen tekijälle Asiantuntijavastausten koostaminen Sivuston sisällön järjestäminen ja muokkaaminen saatujen ehdotusten pohjalta
Tutkimusongelman ja toteutetun ratkaisun kommunikointi	Tutkimustulosten ja ohjesivuston esittely Maanmittauslaitoksen sovelluspalveluiden esimiehille ja palvelupäälliköille Tutkimustulosten ja ohjesivuston esittely Maanmittauslaitoksen tietosuojavastaavalle

Kuva 1.1: DSRM-vaiheet ja niiden toteutuminen tutkimuksessa

vaatimukset numeroitiin ja luetteloitiin. Tämän jälkeen sovellettiin tutkimuskysymyksen vastausta yhdistämällä lakiteksteistä kerätyt numeroidut vaatimukset kokonaisarkkitehtuurisuunnitteluun. Tutkimusosuudessa arvioitiin kokemuspohjaisesti näiden sovelluskehitykseen vaikuttavien vaatimusten yhteyttä TOGAF-kokonaisarkkitehtuurikehyksen [24] ADM-kehittämismallin vaiheistukseen ja muodostettiin tuloksena matriisi, joka kuvaa vaatimusten ja vaiheiden suhdetta toisiinsa (liite A).

Vastausta toiseen tutkimuskysymykseen haettiin edelleen soveltavalla tutkimuksella käyttäen tutkimusmetodina suunnittelututkimuksen (design science) menetelmiin lukeutuvaa Design Science Research Methology (DSRM) -tutkimusmenetelmää [25]. Tutkimustyypille olennaista on ratkaista tutkimuksessa kuvattu ongelma ja tuottaa lopputuloksena uusi artefakti kuten tuote (tietojärjestelmä tai sovellus), toteutustekniikka tai -teknologia sekä malli tai menetelmä. DSRM-menetelmän tutkimusprosessi on jaettu kuuteen vaiheeseen. Tutkimuksen toteuttaminen DSRM-prosessin mukaisesti on esitelty kuvassa 1.1.

Tutkimuksen lopputuloksena syntyi tämän tutkielman artefakti eli kappaleessa 5.3 kuvattu **Maanmittauslaitokselle tehty sovelluskehityksen tietosuojaohjeistusrunko**. Tutkielman alussa taustatutkimuksessa kerätyt vaatimusluettelot muodostavat ohjeistukseen tarkistuslistoja, joiden avulla voidaan arvioida tapauskohtaisesti tietojärjestelmäkehityksessä tarvittavat tietosuojatoimenpiteet. Maanmittauslaitoksessa toteutettiin vuosina 2016–2018 kaksi tietosuoja-asetukseen liittyvää projektia, joissa selvitettiin asetuksen organisaatiolle asettamia vaatimuksia ja suunniteltiin niiden täytäntöönpanoa. Nyt toteutettu tietosuojaohjeistusrunko oli yksi projektien loppuraporteihin kirjatuista tulevaisuuden toteutustarpeista.

Tutkimusten lopputulosten jakaminen Maanmittauslaitoksen sovelluskehityksen toimijoille tehdään tutkimuksen jälkeen organisaation sovelluskehityksestä vastaavan johdon valitsemalla tavalla.

1.3 Aineisto

Tutkielmassa tukeuduttiin pääosin yleiseen tietosuojaoikeudelliseen oikeuskirjallisuuteen eli lakiteksteihin. Tutkielman tärkeimpänä lähteenä käytettiin EU:n yleistä tietosuoja-asetusta (EU) 2016/679 [7]. Muita tärkeitä oikeustieteellisiä lähteitä olivat tietosuojalaki 1050/2018 [29], laki viranomaisen toiminnan julkisuudesta 621/1999 [19] ja laki julkisen hallinnon tiedonhallinnasta 906/2019 [17]. Kyseiset lähteet toimivat perustana tutkimustyölle.

Menetelmällisenä lähteenä käytettiin TOGAF-nimellä tunnettua The Open Group Architecture Framework –kokonaisarkkitehtuurikehystä [24], josta tutkimuksessa hyödynnettiin siinä kuvattua arkkitehtuurikehittämisen prosessimallia.

Tutkielman otsikossa olevaa käsitettä Privacy by Design avattiin sen julkaisseen Ann Cavoukianin artikkelin ”Privacy by design” (2009) [1], Danezis et al. artikkelin ”Privacy and Data Protection by Design – from policy to engineering” (2015) [3] ja van Rest et al. artikkelin ”Designing Privacy-by-Design” (2014) [26] avulla. Kyseiset artikkelit taustoittavat käsitettä ja selventävät sen merkitystä tietosuoja-asetuksessa.

Näiden lähteiden lisäksi tutkimuksessa hyödynnettiin vähäisissä määrin valtionhallinnossa tehtyjä raportteja, jotka liittyvät tietosuojaan, sekä muutamaa tieteellistä artikkelia. Lähdemateriaalina on myös toki mainittava tutkimuksen kohteena olevan Maanmittauslaitoksen tietosuojaprojektimateriaalit vuosilta 2016–2018 [22].

Hyvin suuri osa tutkielmassa tehdyistä päätelmistä pohjautuu sen kirjoittajan yli 30-vuotiseen kokemukseen it-alalta niin sovellus- kuin menetelmäkehityksen alueelta.

1.4 Tutkielman rakenne

Tämän tutkielman ensimmäiseen asiakappaleeseen, kappaleeseen 2, on referoitu tietosuoja-asetuksen yleiset piirteet sekä määritelty sovelluskehityksen kannalta oleellisimmat tietosuoja-asetuksen käyttämät termit. Lisäksi kappaleessa on esitelty muita henkilötietojen käsittelyyn vaikuttavia lakeja.

Kappaleessa 3 on ensin selvitetty sisäänrakennetun tietosuojan periaatteet ja tämän jälkeen käyty läpi tietosuoja-asetuksen ja muun lainsäädännön ne kohdat, jotka asettavat vaatimuksia sisäänrakennetun tietosuojan toteuttamiselle organisaation tietojärjestelmiin. Kustakin kohdasta on listattu tietosuojavaatimukset sovelluskehitykselle.

Seuraavassa kappaleessa 4 edellä listatut tietosuojavaatimukset on kiinnitetty TOGAF-arkkitehtuuriviitekehyksen arkkitehtuurin kehittämissyklin vaiheisiin ja tulkittu niiden vaikutusta sovelluskehityksessä tehtäviin valintoihin.

Tutkielman toimintatutkimuksen kohde, Maanmittauslaitos, on esitelty kappaleessa 5. Kappaleeseen on koostettu yhteenveto tutkimustyön aikana tehdyistä Maanmittauslaitoksen asiantuntijoiden haastatteluista liittyen tietosuojavaatimusten ohjeistustarpeisiin sekä kuvattu haastattelutulosten perusteella toteutettu ohjerunko, joka on toteutettu Maanmittauslaitoksen sovelluskehityksen tarpeisiin. Kappaleen lopussa on arvioitu toteutettua ohjeistusta ja sen soveltuvuutta Maanmittauslaitoksen käyttöön.

Tutkielman toiseksi viimeisessä kappaleessa 6 on pohdittu tutkimuksen onnistumista ja siitä saatuja oppeja sekä mahdollisia jatkotutkimusaiheita. Viimeisessä kappaleessa 7 tehdään yhteenveto tutkielmasta ja sen lopputuloksesta.

2 EU:n yleinen tietosuoja-asetus

EU:n yleinen tietosuoja-asetus 2016/679 [7] annettiin 27.4.2016, ja se tuli velvoittavaksi kaikissa EU-jäsenmaissa 25.5.2018. Asetus määrää luonnollisten henkilöiden, toisin sanoen EU-jäsenmaiden kansalaisten ja muiden EU:n alueella oleskelevien ja asioivien henkilöiden, henkilötietojen käsittelyn periaatteista. Kantavana ajatuksena on luonnollisten henkilöiden suojelu määrittämällä henkilötietojen käsittelyyn liittyvät oikeudet, vapaudet ja velvollisuudet yhdenmukaisesti, kattavasti ja EU:n laajuisesti. Tietosuoja on EU-kansalaisen perusoikeus. Kaikki henkilötieto ei kuitenkaan ole aina automaattisesti suojeltavaa, vaan kutakin tietoa on tarkasteltava sen mukaisesti, missä yhteydessä se ilmenee [7](1 artikla).

Tässä kappaleessa käydään läpi tietosuoja-asetuksen tärkeimmät termit ja sen pääkohdat.

2.1 Henkilörekisteri, rekisteröity ja rekisterinpitäjä

Tietosuoja-asetuksella säädellään luonnollisten henkilöiden henkilötietojen käsittelyä ja rekisteröintiä henkilörekistereihin.

Henkilörekisterillä tarkoitetaan mitä tahansa sellaista henkilötietoja sisältävää tietojoukkoa, jossa tiedot ovat järjestetyssä muodossa ja josta tietoja voi etsiä näiden henkilötietojen avulla. Henkilörekisterillä ei ole muita muotovaatimuksia. Tietosuoja-asetuksessa on kuitenkin tehty rajaus, ettei sitä sovelleta sellaisiin asiakirjoihin tai asiakirjakokoelmiin, ”joita ei ole järjestetty tiettyjen perusteiden mukaisesti”. Tätä rajausta voidaan tulkita niin, että mikäli henkilötietoja sisältävien asiakirjojen tai muiden henkilötietoja sisältävien tietojen joukosta ei ole mahdollista löytää täsmällisesti tietyn rekisteröidyn tietoja, eivät kyseiset asiakirjat tai tietojoukot kuulu tietosuoja-asetuksen piiriin. [7](4 artikla)

Henkilötietojen käsittelyyn liittyy olennaisesti kolme roolia: rekisteröity, rekisterinpitäjä ja henkilötiedon käsittelijä [7](4 artikla).

Rekisteröidyksi henkilöksi (tai lyhyemmin rekisteröidyksi) kutsutaan sitä luonnollista henkilöä, johon henkilörekisteriin kirjatut henkilötiedot liittyvät. Tietosuoja-asetuksen pääajatuksena on tämän rekisteröidyn tietojen suojeleminen ja hänen oikeuksistaan huo-

lehtiminen.

Rekisterinpitäjä on luonnollinen henkilö tai organisaatio, jonka vastuulla tiedot sisältävä henkilörekisteri sekä siihen kirjattujen henkilötietojen käsittelyn lainmukaisuus on. Rekisterinpitäjän tehtävänä on määritellä henkilörekisterin tarkoitus ja tavat, joilla näitä tietoja on lupa käsitellä.

Henkilötietojen käsittelijä puolestaan on henkilö, joka henkilörekisteriin tallennettuja tietoja käsittelee, tai organisaatio, joka toteuttaa henkilötietojen käsittelyä rekisterinpitäjän puolesta. Rekisterinpitäjän on siis mahdollista käyttää myös ulkopuolisia henkilötietojen käsittelijöitä suorittamaan käsittelyä sen lukuun. Jokainen käsittelijä on omalta osaltaan vastuussa siitä, että henkilötietoja käsitellään lain ja rekisterinpitäjän ohjeiden mukaisesti. Henkilörekisterien sisältämiä tietoja on oikeus käsitellä vain työtehtäviin liittyen.

2.2 Henkilötiedon käsite

Tietosuoja-asetusta sovelletaan vain asetuksessa tarkoitettujen henkilötietojen käsittelyyn. Termi **henkilötieto** on määritelty tietosuoja-asetuksessa [7](4 artikla) seuraavasti:

"'Henkilötiedoilla' [tarkoitetaan] kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella."

Tietosuoja-asetuksen mukaan ainoastaan sellainen tieto, jota hyödyntämällä henkilö on tunnistettavissa, katsotaan tietosuojan piirissä olevaksi henkilötiedoksi [7]. Asetuksen tietosuojaperiaatteita on sovellettava kaikkiin näihin tietoihin. Poikkeuksena tähän ovat kuolleet henkilöt, joihin liittyviin tietoihin ei tietosuoja-asetusta sovelleta, ellei siitä ole erikseen säädetty kansallisella lainsäädännöllä.

Henkilö voidaan tunnistaa henkilötiedon avulla suoraan tai epäsuorasti. Mikäli henkilön voi suoraan ja yksiselitteisesti tunnistaa kyseisen tiedon avulla, on kyseessä **suora henkilötieto**. Näitä suoria henkilötietoja ovat tai voivat olla muun muassa nimi, henkilötunnus, kotiosoite, sähköpostiosoite, mobiilipuhelinnumero ja ip-osoite sekä tietyt biologiset tunnisteet kuten sormenjälki tai näytteistä kerätyt geneettiset tiedot. Jos taas yh-

distämällä tietoa muihin tietoihin henkilö on mahdollista tunnistaa, silloin kyseessä on **epäsuora henkilötieto**. Tämän tyyppisiä henkilötietoja ovat esimerkiksi auton rekisteritunnus, kiinteistötunnus ja käyttäjätunnus sekä paikkatiedot ja tieliikennepalveluista saatavat metatiedot. Myös valokuvaa tulee käsitellä epäsuorana henkilötietona, mikäli siinä esiintyvät henkilöt ovat kuvan perusteella tunnistettavissa. Epäsuoraa tunnistamista on lisäksi mahdollista tehdä esimerkiksi sukupuoli-, ikä-, työtehtävä- ja/tai oppiarvotietoja yhdistämällä.

Oleellista onkin arvioida, onko henkilö tunnistettavissa niiden tietojen perusteella, joita hänestä henkilörekisteriin rekisteröidään. Tässä yhteydessä on harkittava ja tarvittaessa selvitettävä, onko olemassa keinoja, joita käyttämällä henkilö olisi kyseisistä tiedoista kohtuullisen todennäköisesti tunnistettavissa joko suoraan tai epäsuorasti. Tällaisia keinoja ovat muun muassa julkiset tai kaupalliset palvelut, joista on mahdollista etsiä henkilön tietoja esimerkiksi nimellä, syntymäajalla, auton rekisteritunnuksella tai puhelinnumerolla. Samoin on harkittava, ovatko tunnistustyöstä aiheutuvat kustannukset tai siihen käytettävä aika sikäli kohtuullisia, että voitaisiin pitää todennäköisenä, että tiedon tai tietojen perusteella olisi odotettavissa pyrkimyksiä selvittää rekisteröity niiden perusteella. Mikäli voidaan todeta, ettei tietoja todennäköisesti tulla käyttämään tunnistamisessa, koska se vaatii enemmän kuin kohtuullista vaivannäköä, siinä tapauksessa niitä ei käsitellä henkilötietoina.

Tämän vuoksi vain harvoja, aina selkeästi henkilön yksilöiviä tietoja kuten henkilötunnus on mahdollista määritellä varmasti henkilötiedoiksi. Muiden tietojen osalta joudutaan siis aina ensin tapauskohtaisesti harkitsemaan, onko tieto henkilötietoa tietosuoja-asetuksen määrittelyn mukaisesti. Esimerkiksi henkilön nimi on nopeasti ajateltuna henkilötieto, mutta mikäli nimi on yleinen ja se esiintyy yhteydessä, jossa saman nimisiä henkilöitä on todennäköisesti useita, silloin se ei yksinään riitä henkilön tunnistamiseen. Vasta kun nimeen liitetään jokin muu tieto, jonka avulla henkilö voidaan epäsuorasti tunnistaa, tekee se siitä henkilötiedon. Näiden muiden epäsuoran tunnistamisen mahdollistavien tietojen ei tarvitse olla rekisterinpitäjän hallussa, vaan niiksi voidaan myös lukea tietoja, jotka ovat muualta selvitettävissä ja yhdistettävissä kyseisen henkilörekisterin tietoihin.

Myös paikkatieto voi olla henkilötietoa [15]. Paikkatieto on sijaintiin kiinnitettyä tietoa, joka jakautuu välilliseen (koordinaatit) ja välittömään (osoite, tunnus, paikannimi) paikkatietoon ja johon liittyy sijaintitiedon lisäksi ominaisuustieto, joka kuvaa sijainnissa olevaa kohdetta. Paikkatiedosta on tapauskohtaisesti mietittävä, onko kyseessä henkilötieto. Jos paikkatiedon avulla on mahdollista tunnistaa henkilö joko suoraan tai

epäsuorasti yhdistämällä paikkatieto muihin henkilön paljastaviin tietoihin, silloin sitä tulee käsitellä henkilötietona. Esimerkiksi osoitetieto tai kiinteistöä kuvaavat muut tunnisteet sekä rakennus- tai olosuhdetiedot voivat olla asunnon tai kiinteistön omistajan tai mahdollisen vuokralaisen henkilötietoja, kun ne ovat kontekstissa, jossa ne paljastavat rekisteröidyn. Sen sijaan karttatietoja kuten osoitteita kartassa ei pidä käsitellä henkilötietoina niiden yleishyödyllisyydestä johtuen.

2.3 Yleistä tietosuoja-asetuksesta

Henkilötieto tarkoittaa siis luonnolliseen henkilöön liittyvää tietoa, jonka avulla henkilö on mahdollista tunnistaa joko suoraan kyseisen tiedon perusteella tai epäsuorasti yhdistämällä henkilötietoja toisiinsa [7](1 artikla). **Henkilötietojen käsittelyksi** luetaan sellaiset osittain tai kokonaan automaattisen tietojenkäsittelyn avulla suoritettavat tai henkilötietojen käsittelijän manuaalisesti suorittamat toiminnot, jotka kohdistuvat henkilötietoihin tai henkilörekistereihin [7](4 artikla). Tietosuoja-asetuksessa on nimetty seuraavat henkilötietojen käsittelytoiminnot:

- tietojen kerääminen, tallentaminen, säilyttäminen, muokkaaminen ja muuttaminen
- tietojen järjestäminen, jäsentäminen, käyttö, haku ja kysely
- tietojen yhteensovittaminen ja yhdistäminen
- tietojen siirtäminen ja luovuttaminen kolmansille osapuolille
- tietojen rajoittaminen, poistaminen ja tuhoaminen.

Huomionarvoista on, että tietosuoja-asetuksen vaatimukset kohdistuvat vain sellaisiin henkilötietoihin, jotka joko jo kuuluvat henkilörekisteriin tai jotka on tarkoitus liittää rekisterin osaksi.

Jotta henkilötietojen käsittely olisi yhdenmukaista kaikissa EU:n jäsenvaltioissa, on asetukseen kirjattu määritelmiä ja sääntöjä liittyen seuraaviin aihealueisiin:

- Rekisteröidyn oikeudet
- Henkilötietoja käsittelevien velvollisuudet
- Henkilötietojen käsittelystä päättävien velvollisuudet

- Henkilötietojen käsittelyä valvovien valtuudet
- Sääntöjen rikkomisesta seuraavat sanktiot

Tietosuoja-asetuksen vaatimukset koskevat kaikkea sellaista henkilötietojen käsittelyä, jota suorittaa rekisterinpitäjä tai henkilötietojen käsittelijä, jolla on toimipaikka ja toimintaa EU:n alueella. Sillä, suoritetaanko henkilötietojen käsittely todellisuudessa EU:n alueella, ei ole merkitystä. Asetus koskee myös organisaatioita, joilla ei ole toimipaikkaa EU:n alueelle, mutta jotka tarjoavat tuotteita tai palveluita EU-alueelle tai keräävät tietoa EU:n alueella olevien henkilöiden käyttäytymisestä [7](3 artikla). Yrityksille, joiden koko on alle 250 työntekijää, on asetuksessa määritelty tiettyjä helpotuksia velvoitteisiin [7](30 artikla). Lisäksi asetuksen piiristä on rajattu pois henkilötietojen käsittely, joka liittyy EU:n yhteiseen ulko- ja turvallisuuspolitiikkaan sekä toimivaltaisten viranomaisten rikoksiin, turvallisuusuhkiin ja niiden ehkäisemiseen liittyviin tehtäviin. Asetus ei myöskään velvoita yksityishenkilöitä toimimaan asetuksen vaatimusten mukaisesti: henkilökohtaisia tai kotitalouden tarpeita varten on edelleen täysin sallittua kerätä henkilötietoja [7](2 artikla).

Rekisteröidylle on annettu tietosuoja-asetuksessa oikeuksia kuten oikeus saada pääsy omiin henkilötietoihinsa ja oikeus pyytää tiedot poistetuksi, joiden avulla hänellä on mahdollisuus vaikuttaa omien henkilötietojensa käsittelyyn. Rekisteröidyn oikeuksia käsitellään tarkemmin kappaleessa 3.3. Rekisterinpitäjä saa kerätä henkilötietoja ainoastaan silloin, kun siihen on olemassa tietosuoja-asetukseen erikseen määritelty lain mukainen peruste. Tämä henkilötietojen käsittelyn oikeusperuste vaikuttaa siihen, minkälaisia oikeuksia rekisteröidyllä henkilöllä lopulta on rekisteröityihin tietoihin. Näitä oikeusperusteita ovat muun muassa rekisteröidyn suostumus, sopimukseen perustuva rekisteröinti ja rekisterinpitäjän lakisääteinen velvoite. Esimerkiksi mikäli rekisteröinti perustuu lakisääteiseen velvoitteeseen, ei rekisteröidyllä välttämättä ole oikeutta käyttää kaikkia oikeuksiaan.

Henkilötietojen käsittelyssä on noudatettava seuraavia yleisiä periaatteita [7](5 artikla):

- Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi (lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate)
- Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten (käyttötarkoitussidonnaisuuden periaate)
- Henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja niihin tietoihin, jotka ovat tarpeellisia suhteessa niiden käyttötarkoitukseen (tietojen minimoinnin periaate)

- Henkilötietojen tulee olla täsmällisiä ja ajantasaisia, ja epätarkat ja virheelliset tiedot tulee voida oikaista tai poistaa kohtuullisin toimenpitein ja viipymättä (täsmällisyyden periaate)
- Henkilötietoja ei tule säilyttää siinä muodossa, että niistä tunnistaa henkilön, sen pitempään kuin mikä on tietojenkäsittelyn vuoksi välttämätöntä (säilytyksen rajoittamisen periaate)
- Henkilötietojen käsittelyssä on varmistettava niiden asianmukainen turvallisuus kuten tietojen suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta teknisin ja organisatorisin toimin (eheyden ja luottamuksellisuuden periaate)

Rekisterinpitäjä on vastuussa rekisteröityjen henkilöiden oikeuksien toteutumisesta ja mainittujen käsittelyperiaatteiden noudattamisesta [7](24 artikla). Rekisterinpitäjä vastaa joko teknisin keinoin tai organisatorisin toimin siitä, että henkilörekisterit ovat tietoturvallisia ja käsittelytoimenpiteet suoritetaan asetuksen periaatteiden mukaisesti. Rekisterinpitäjälle on tietosuoja-asetuksessa määritetty osoitusvelvollisuus, jonka mukaan rekisterinpitäjän on kyettävä myös näyttämään toteen, että periaatteita on noudatettu kaikessa sen toiminnassa. Seloste käsittelytoimista on tietosuoja-asetuksessa erikseen mainittu dokumentti, joka osaltaan toimii osoitusvelvollisuuden ja rekisteröidyn oikeuksien täyttäjänä [7](30 artikla). Rekisterinpitäjällä on velvoite tehdä tietosuojaseloste kaikista henkilörekistereistä. Selosteeseen kirjataan kyseisen rekisterin henkilötietojen käsittelyyn liittyvät periaatteet kuten säilytettävät tiedot, niiden käyttötarkoitus, säilytysaika, säännölliset tiedonluovutukset ja rekisteriin kohdistetut tietoturvatoimenpiteet. Selostetta käsittelytoimista kutsutaan usein myös **tietosuojaselosteeksi**.

Rekisterinpitäjän velvollisuutena on ohjeistaa henkilörekisterien käsittely ja huolehtia siitä, että kaikki henkilötietojen käsittelijät osaavat toimia ohjeiden mukaisesti. Mikäli tietojen käsittelyssä käytetään rekisterinpitäjän henkilökunnan ulkopuolisia henkilötietojen käsittelijöitä, on rekisterinpitäjän mahdollisuuksien mukaan varmistuttava heidän osaamisestaan ja luotettavuudestaan sekä siitä, että henkilötietojen käsittelijä on suojannut henkilötiedot tietosuoja-asetuksen vaatimusten mukaisesti ja noudattaa asetuksen määräyksiä [7](28 artikla). Henkilötietoja rekisterinpitäjän lukuun käsittelevän organisaation on toimittava rekisterinpitäjän antamien ohjeiden mukaan ja huolehdittava henkilökuntansa sitoutumisesta ohjeisiin ja salassapitovelvollisuuteen. Henkilötietojen käsittelystä rekisterinpitäjän lukuun sovitaan erillisellä sopimuksella, johon kirjataan käsiteltävät henkilötiedot,

käsittelyn tyyppi ja toimeksiannon kesto sekä henkilötietojen käsittelijän vastuut ja toimenpiteet sopimuksen päättyessä. Henkilötietojen käsittelijä ei saa käyttää alihankkijoita ilman rekisterinpitäjän lupaa. Ulkopuolisella henkilötietojen käsittelijällä on tyypillisesti myös velvollisuus poistaa tai palauttaa henkilötiedot rekisterinpitäjälle sopimuksen päätyttyä. Tätä rekisterinpitäjän ja ulkopuolisen henkilötietojen käsittelijän välistä sopimusta varten on laadittu EU:n vakiosopimuslausekkeita helpottamaan sopimuksen tekemistä. [7](29 artikla)

Myös ulkoisen sovellustoimittajan sovelluskehittäjät, joilla on pääsy rekisterinpitäjän henkilörekisteriin, ovat ulkopuolisia henkilötiedon käsittelijöitä. Näitä yrityksiä koskee samat vaatimukset kuin sellaisia ulkopuolisia henkilötietojen käsittelijäorganisaatioita, jotka suorittavat varsinaisia henkilötietojen käsittelytehtäviä. Jos sovellustoimittajan henkilöstöllä on pääsy asiakasorganisaationsa henkilörekistereihin, on myös heidän kanssaan tehtävä tästä sopimus.

Rekisterinpitäjälle on asetettu tietosuoja-asetuksessa tiettyjä ilmoitusvelvollisuuksia. Rekisterinpitäjällä on muun muassa velvollisuus ilmoittaa rekisteröidylle hänen tietojensa rekisteröinnistä, jos tiedot saadaan muualta kuin rekisteröidyltä itseltään [7](14 artikla). Lisäksi rekisterinpitäjällä on velvollisuus ilmoittaa havaitusta henkilötietojen tietoturvaloukkauksesta viipymättä sekä kansalliselle valvontaviranomaiselle että rekisteröidylle, jonka henkilötiedot ovat joutuneet tietoturvaloukkauksen kohteeksi [7](33 ja 34 artikla). Ilmoitusvelvollisuutta käsitellään tarkemmin kappaleissa 3.3 ja 3.6.1.

Mikäli rekisteröidylle koituu vahinkoa asetuksen periaatteiden rikkomisesta tietojenkäsittelyn yhteydessä, on rekisterinpitäjä tai henkilötietojen käsittelijä velvollinen korvaamaan vahingon rekisteröidylle, ellei kyetä osoittamaan, ettei vahinko ole ollut rekisterinpitäjän tai henkilötietojen käsittelijän aiheuttama [7](83 artikla).

2.4 Tietosuoja-asetuksen toteutumisen valvonta ja sanktiot

Kuten edellä todettiin, on yksi rekisterinpitäjän velvollisuuksista ilmoitusvelvollisuus henkilötietojen tietoturvaloukkauksista kansalliselle valvontaviranomaiselle. Kyseinen valvontaviranomainen on jäsenvaltion nimittämä riippumaton viranomainen, joka käyttää jäsenvaltiossa ylintä toimivaltaa tietosuoja-asioissa [7](51 artikla). Valvontaviranomaisia voi tarvittaessa olla jäsenvaltiossa enemmän kuin yksi. Valvontaviranomaisen tehtäviä

ovat muun muassa rekisteröityjen tekemien valitusten käsittely, asetuksen soveltamista koskevien tutkimusten suorittaminen sekä yleisen tietosuojatietoisuuden lisääminen. Valvontaviranomaisella on myös valtuudet asettaa tarvittaessa väliaikainen tai pysyvä tietojenkäsittelyn rajoitus rekisterinpitäjälle sekä määrätä hallinnollisia sakkoja. Kansallisen valvontaviranomaisen tehtävistä on tarkemmin säädetty tietosuoja-asetuksessa [7](57 artikla).

Sekä rekisterinpitäjä- että henkilötiedon käsittelijä -organisaatioissa tietosuojan toteutumista valvoo tietosuojavastaava [7](37 artikla). Tietosuojavastaava tulee nimittää, jos organisaatio on viranomainen tai sen ydintehtäviin liittyy henkilötietojen rekisteröintiä ja käsittelyä. Tietosuojavastaavan olennaisimpia tehtäviä on organisaation ohjaaminen tietosuojaan liittyvissä kysymyksissä sekä tietosuoja-asetuksen toteutumisen valvonta. Tehtävistä on tarkemmin säädetty tietosuoja-asetuksessa [7](39 artikla). Tietosuojavastaavan ei tarvitse olla organisaation omaa henkilökuntaa, vaan hänet voidaan nimittää myös organisaation ulkopuolelta. Tietosuojavastaavan tueksi on toivottavaa nimetä tietosuojaorganisaatio. Organisaation tietosuojavastaavan yhteystiedot ovat julkista tietoa ja ne ilmoitetaan muun muassa tietosuojaselosteessa, ja rekisteröidyillä onkin oikeus ottaa tietosuojavastaavaan yhteyttä kaikissa asioissa, jotka liittyvät heidän henkilötietojensa rekisteröintiin kyseisessä organisaatiossa.

Tietosuoja-asetuksessa on määritetty hallinnollinen seuraamusmaksu, jota voidaan käyttää sanktiona tietosuojarikkomuksiin liittyen [7](83 artikla). Tämä on kokonaan uusi asia verrattuna aiempaan henkilötietolakiin. Maksu voi olla suurimmillaan 20 miljoonaa euroa tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta kokonaisliikevaihdosta. Tämän hallinnollisen sakon määräämisessä tulee ottaa huomioon muun muassa rikkomuksen vakavuus ja tahallisuus sekä rekisterinpitäjän tai henkilötietojen käsittelijän toimenpiteet rekisteröidylle koituvan haitan pienentämiseksi. Lievempiä seuraamuksia ovat esimerkiksi varoitus, huomautus ja valvontaviranomaisen määräämät toimenpiteet kuten käsittelyn rajoitus [7](58 artikla).

Rekisteröidyillä on oikeus nostaa kanne rekisterinpitäjää, henkilötiedon käsittelijää tai valvontaviranomaista kohtaan liittyen henkilötietojen käsittelyyn tai siitä tehtyihin viranomaispäätöksiin [7](78 ja 79 artikla).

2.5 Tietosuojalaki ja muu henkilötietojen käsittelyyn vaikuttava lainsäädäntö

EU:n asetukset ovat suoraan sovellettavaa lainsäädäntöä, eli ne ovat sellaisenaan voimassa jäsenvaltioissa toisin kuin direktiivit, jotka aina vaativat kansallisen toimeenpanevan lainsäädännön. Tietosuoja-asetukseen on kuitenkin erikseen kirjattu, mitä asetuksen kohtia on oikeus täydentää ja täsmentää kansallisella lainsäädännöllä. Jäsenvaltioilla on tämän lisäksi olemassa omaa alakohtaista lainsäädäntöä, jolla on vaikutusta tietosuojaan. Tietosuoja-asetuksessa mainitaan erikseen oikeus- ja turvallisuusviranomaiset, joiden toimista on mahdollista säätää alakohtaisella lainsäädännöllä.

Tietosuojalaki 1050/2018 [29] astui Suomessa voimaan 1.1.2019. Laissa on muun muassa määrätty, että Suomessa tietosuoja-asetuksessa mainittuja kansallisen valvontaviranomaisen tehtäviä hoitaa oikeusministeriön yhteydessä toimiva tietosuojavaltuutettu. Lisäksi laissa on todettu, että henkilötietojen käsittelijällä on aina vaitiolovelvollisuus näkemistään henkilötiedoista. Henkilötietojen käsittelyä ohjaa alaikäisen henkilön rekisteröinnin ikäraja: jos rekisteröinti perustuu suostumukseen, saa lapsen tiedot saa tarvittaessa rekisteröidä henkilörekisteriin vain, jos tämä on vähintään 13-vuotias. Tämä ei kuitenkaan koske muita rekisteröinnin oikeusperusteita. Erityisryhmien henkilötietojen käsittelystä on säädetty tietosuojalaissa siitä, missä tilanteissa näihin erityisryhmiin kuuluvien henkilöiden henkilötietojen käsittely on sallittua.

Suomalaisittain erityisen tärkeä on tietosuojalain ohjeistus liittyen henkilötunnuksen käsittelyyn. Siitä on todettu, että se on sallittua vain rekisteröidyn suostumuksella tai mikäli käsittelystä on erikseen säädetty laissa. Lisäksi se on sallittua, jos rekisteröidyn yksiselitteinen tunnistaminen on välttämätöntä lakisääteisen tehtävän suorittamiseksi, rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteutumiseksi tai historiallista, tieteellistä tai tilastollista tutkimusta varten. Sitä saa myös käsitellä rahaan ja sosiaali- ja terveyssektoriin liittyvissä tehtävissä sekä palvelussuhteisiin liittyen. Henkilötunnusta ei kuitenkaan saa merkitä tulosteisiin tai muihin asiakirjoihin, ellei se ole nimenomaisesti tarpeellista.

Tietosuojalaissa on myös otettu kantaa rekisteröityjen oikeusturvaan ja mahdollisiin tietosuojarikkomuksiin liittyviin seuraamuksiin sekä muutoksenhakuun liittyviin yksityiskohtiin. Sananvapauden ja tiedonvälityksen vapauden turvaamiseksi on todettu ne tietosuoja-asetuksen kohdat, joita ei journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun

nimissä ole tarvetta noudattaa. Vastaavasti laissa on säädetty tieteellisiä ja historiallisia tutkimustarkoituksia taikka tilastollisia tai yleisen edun mukaisia arkistointitarkoituksia varten tehtävään henkilötietojen käsittelyyn liittyvistä poikkeuksista ja niihin liittyvistä ehdoista.

Lisäksi tietosuojalaissa rajataan rekisteröidyn oikeutta saada tietoja henkilörekisterissä olevista omista henkilötiedoistaan tilanteissa, joissa tiedon antamisesta olisi haittaa yleiselle turvallisuudelle, rekisteröidylle itselleen tai viranomaisten suorittamille valvonta- ja tarkastustehtäville.

Muita kansallisia henkilötietojen käsittelyä sääteleviä lakeja ovat julkisuuslaki ja laki yksityisyyden suojasta työelämässä.

Laki viranomaisen toiminnan julkisuudesta 621/1999 eli **julkisuuslaki** [19] säätää kansalaisten ja organisaatioiden oikeudesta saada tietoa viranomaisten julkisista asiakirjoista. Tämä vaikuttaa viranomaisissa myös henkilötietojen käsittelyyn. Julkisuusperiaatteen mukaisesti viranomaisten asiakirjat ovat lähtökohtaisesti julkisia, ja mikäli asiakirja on salassa pidettävä, on siitä säädetty laissa erikseen. Jokaisella on oikeus saada tieto julkisista asiakirjoista sekä lisäksi itseään koskevista asiakirjoista tietyin rajoituksin. Asiakirjan pyytäjän täytyy osata yksilöidä haluamansa asiakirja riittävän hyvin, jotta viranomainen voi selvittää, mitä asiakirjaa pyyntö koskee. Lisäksi viranomaisten rekistereistä voidaan luovuttaa henkilötietoja otteina, kopioina tai sähköisessä muodossa erillisestä pyynnöstä. Pyytäjällä tulee olla lain mukainen oikeus tietoihin, ja hänen tulee tehdä selvitys tietojen käyttötarkoituksesta. Rekisterinpitäjä on kuitenkin tässäkin tilanteessa velvollinen noudattamaan tietosuojaperiaatteita. Suoramarkkinointiin tai mielipide- ja markkinatutkimuksiin henkilötietoja saa luovuttaa vain, jos siitä on erikseen säädetty tai jos rekisteröidyltä on saatu siihen suostumus. Tietosuoja-asetuksessa on todettu, että sitä sovellettaessa huomioidaan kansalliset virallisten asiakirjojen julkisuuteen liittyvät periaatteet.

Laissa yksityisyyden suojasta työelämässä 759/2004 [20] on säädetty työnantajaan palvelussuhteessa olevien henkilöiden henkilötietojen käsittelystä. Laki on ollut voimassa 1.10.2004 alkaen. Lain mukaan työnantaja saa kerätä palvelussuhteisesta henkilöstä vain ne tiedot, jotka ovat oleellisia työsuhteen kannalta, ja ne tulee pyytää ensisijaisesti työntekijältä itseltään tai pyydettävä tältä erillinen suostumus tietojen keräämiseen muualta. Työntekijöiden terveydentilaa koskevia henkilötietoja ei saa säilyttää muiden henkilötietojen yhteydessä, eikä niitä saa käsitellä kuin henkilöt, joiden tehtävänkuvaan se kuuluu. Terveydentilaa koskevat tiedot on myös poistettava heti, kun niille ei ole enää tarvetta. Myös kamera- ja kulunvalvonnassa sekä esimerkiksi tietoverkon käytön valvon-

nassa syntyy rekisteröitäviä henkilötietoja, joista työnantajalla on velvollisuus informoida työntekijöitä.

Viimeisin voimaan tullut kansallinen laki, jolla on vaikutusta henkilötietojen käsittelyyn, on 1.1.2020 voimaan tullut laki julkisen hallinnon tiedonhallinnasta 906/2019 eli niin kutsuttu **tiedonhallintalaki** [17]. Kyseisen lain tavoitteena on varmistaa viranomaisten tietoaineistojen yhdenmukainen ja tietoturvallinen hallinta sekä aineistojen turvallinen ja tehokas hyödyntäminen. Laki asettaa vaatimuksen tiedonhallintamallista, jonka avulla pyritään muun muassa vähentämään päällekkäisiä tiedonkeruita ja parantamaan tietojärjestelmien ja tietovarantojen yhteentoimivuutta. Tiedonhallintamallin tulee sisältää kuvaukset toimintaprosesseista, tietovarannoista ja niiden yhteyksistä prosesseihin ja tietojärjestelmiin sekä tietosuojaselosteen tietovarantojen sisällöstä, tietoaineistojen arkistoinnista, tietojärjestelmistä ja niiden välisistä yhteyksistä sekä tietoturvallisuustoimenpiteistä. Tämä tukee hyvin tietosuoja-asetuksen asettamaa osoitusvelvollisuutta. Tiedonhallintalaki vaatii organisaatiolta tietoaineistoilta ja tietojärjestelmiltä vikasietoisuutta ja toiminnallista käytettävyyttä sekä tietoturvallisuutta asiakirjojen julkisuuden kuitenkaan estymättä. Asiakirjat tulee säilyttää sähköisessä muodossa ja niiden luotettavuudesta on huolehdittava. Tietojärjestelmiin saa olla käyttöoikeudet vain työtehtävien suorittamiseksi, ja tietojärjestelmien käytöstä ja niistä tehtävistä tiedonluovutuksista tulee kerätä lokia. Lisäksi tietopyynnöt tulee rekisteröidä aina asiarekisteriin eli diaariin.

Tiedonluovutuksiin liittyen tiedonhallintalaki asettaa joitakin vaatimuksia. Tietoaineistoja on pyrittävä hyödyntämään myös viranomaisten välillä teknisen tiedonsiirtorajapinnan tai katseluyhteyden avulla. Tietoja voidaan luovuttaa viranomaisten lisäksi kolmansille osapuolille, jos vastaanottajalla on siihen lakiin kirjattu oikeus. Tällöin teknisten tiedonsiirtorajapintojen kautta tehtävistä tiedonluovutuksista tulee tapauskohtaisesti varmistaa tietojen tarpeellisuus. Vastaavasti katseluyhteyden kautta tehtävässä tiedonluovutuksessa tulee tietojen haku rajoittaa yksittäisiin tietoihin, joiden tarpeellisuudesta ja käyttötarkoituksesta on varmistuttu. Tietoverkossa tehtävien tiedonsiirtojen tulee tapahtua salattua tai suojattua yhteyttä hyödyntäen, mikäli tietoaineisto on salaista, ja tiedon vastaanottaja täytyy voida tunnistaa. Lisäksi tietojärjestelmälle, jonka kautta viranomaisille tarjotaan mahdollisuus katsella rekisterinpitäjän hallussa olevia henkilötietoja, on asetettu vaatimus havaita normaalista poikkeavat haut.

3 Tietosuoja-asetuksen vaatimukset sovelluskehitykselle

Henkilötietojen käsittelyä säätävät lait asettavat organisaatioille runsaasti velvollisuuksia, joiden siirtäminen käytäntöön jää useassa tapauksessa tietojärjestelmiä kehittävien asiantuntijoiden harteille. Velvollisuuksista voidaan johtaa vaatimuksia, jotka on huomioitava niin organisaation kaikissa arkkitehtuurikerroksissa: niin toiminta- kuin tieto- ja sovellusarkkitehtuureissa sekä teknologia-arkkitehtuurissa. Tietosuoja vaatii paljon myös tietoturvalta. Toiminnalliset ja laadulliset vaatimukset on osattava sisällyttää niin organisaation prosesseihin kuin sovellusten toiminnallisuuteen ja tietojärjestelmien toimintaympäristön kokoonpanoon.

Rekisterinpitäjälle on tietosuoja-asetuksessa vastuutettu useita yleisiä vaatimuksia henkilötietojen käsittelyyn liittyen [7](24 artikla). Nämä vaatimukset vaikuttavat pääasiassa prosesseihin. Rekisterinpitäjä on yksiselitteisesti vastuussa sekä oman henkilökuntansa että sen puolesta henkilötietojen käsittelyä tekevien organisaatioiden käsittelyn oikeellisuudesta ja lainmukaisuudesta. Asetus edellyttää, että rekisterinpitäjä on järjestänyt tietojenkäsittelynsä siten, että asetuksen vaatimukset, tietosuojaperiaatteet ja rekisteröidyn oikeudet tulevat huomioitua. Tämä tarkoittaa sitä, että sovelluskehityksen yhteydessä on aina huolehdittava siitä, että mikäli kehitettävissä tietojärjestelmissä käsitellään henkilötietoja, on toteutus tietosuoja-asetuksen ja muiden tietosuojaan vaikuttavien lakien mukainen huomioiden koko henkilötiedon elinkaaren. Tietosuoja-asetuksessa tästä periaatteesta käytetään nimitystä sisäänrakennettu tietosuoja (Privacy by Design) [7](25 artikla). Rekisterinpitäjän on myös kyettävä osoittamaan, että se on tehnyt kaikki tarvittavat toimenpiteet sen eteen, että asetuksen vaatimukset toteutuvat. Näitä toimenpiteitä tulee tarkastella ja päivittää tarvittaessa.

Tietosuoja-asetuksen rekisterinpitäjälle asettamat velvoitteet, joiden toimeenpanossa tietojärjestelmät ja niihin toteutettavat toiminnalliset ominaisuudet ovat merkittävässä roolissa, on tässä tutkielmassa ryhmitelty seuraaviin kokonaisuuksiin:

1. Rekisteröitävien henkilötietojen tunnistaminen
2. Käsittelyn oikeusperusteen tunnistaminen

3. Arkaluonteisten henkilötietojen tunnistaminen
4. Rekisteröidyn oikeuksien huomioiminen
5. Käsittelyperiaatteiden huomioiminen
6. Henkilötietojen siirtäminen ja luovuttaminen
7. Henkilörekisterien tietoturvan varmistaminen
8. Henkilötietojen tietoturvaloukkausten havaitseminen
9. Osoitusvelvollisuuden täyttäminen

Tässä kappaleessa tutustutaan sisäänrakennetun tietosuojan periaatteisiin ja ryhmitellään tietosuoja-asetuksesta ja muusta henkilötietojen käsittelyyn vaikuttavasta lainsäädännöstä poimittavat vaatimukset yllä olevan jaottelun mukaisesti. Löydetyt vaatimukset on numeroitu mainitun ryhmittelyn mukaisesti. Kappaleessa 4 vaatimukset kiinnitetään kokonaisarkkitehtuurin kehittämismalliin. Vaatimukset ja niiden liittäminen arkkitehtuurikehittämisen vaiheisiin on kuvattu liitteessä A.

3.1 Sisäänrakennettu tietosuoja

Tietosuoja-asetuksessa organisaation vastuulle määritetty **sisäänrakennettu tietosuoja** eli Privacy by Design [7](25 artikla) asettaa selkeästi vaatimuksia organisaation toimintojen lisäksi tietoteknisille ratkaisuille ja nimenomaan sille, että tietosuojavaatimukset huomioidaan lähtökohtaisesti aina, kun tehdään sovelluskehitystä. Asetuksessa sanotaan sisäänrakennetusta tietosuojasta seuraavasti:

”Ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille rekisterinpitäjän on käsittelytapojen määrittämisen ja itse käsittelyn yhteydessä toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten tietojen pseudonymisointi ja tarvittavat suojatoimet, jotta ne saataisiin sisällytettyä käsittelyn osaksi ja jotta käsittely vastaisi tämän asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin.”

Samassa yhteydessä tietosuoja-asetuksessa puhutaan oletusarvoisesta tietosuojasta eli Privacy by Default. Oletusarvoinen tietosuoja on asetuksessa selitetty näin [7](25 artikla):

”Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta.”

Privacy by Design -käsitteen perustana on seitsemän periaatetta, joiden tavoitteena on suojata henkilöiden yksityisyyttä mahdollisimman hyvin [1]. Periaatteet ovat vapaasti suomennettuna seuraavat:

1. Proaktiivinen, ei reaktiivinen – ehkäisevä, ei parantava
2. Tietosuoja oletusarvoisena asetuksena
3. Tietosuoja sisäänrakennettuna toteutukseen
4. Täysi toiminnallisuus – positiivinen summa, ei nollasumma
5. Alusta loppuun turvallisesti – täysi elinkaaren suoja
6. Näkyvissä ja läpinäkyvänä – ollaan avoimia
7. Arvostus käyttäjän yksityisyydelle – huolehdi käyttäjäkeskeisyydestä

Sisäänrakennetun tietosuojan ideana on siis huolehtia henkilötietojen tietosuojasta ennakoivasti jo ennen kuin mitään on tapahtunut. Siksi tietosuojan pitäisi olla niin hyvin implementoituna tietojärjestelmien ja organisaation prosessien kehittämiseen, että sen huomioiminen kehittämisessä on automaattista. Silloin toteutuu oletusarvoinen tietosuoja, jossa rekisteröityjen ei itsensä tarvitse huolehtia henkilötietojensa turvallisuudesta, vaan he voivat luottaa siihen, että rekisterinpitäjä huolehtii niistä heidän puolestaan. Tietosuojan vuoksi ei tarvitse luopua mistään, vaan se on mahdollista toteuttaa tietojärjestelmiin muiden vaatimusten kärsimättä. Kun tietosuoja huomioidaan järjestelmissä jo ennen kuin ensimmäistäkään henkilötietoa on kerätty, pystytään tiedot pitämään turvattuna koko niiden elinkaaren ajan. Kun henkilötietoja vielä käsitellään läpinäkyvästi, vahvistaa tietosuoja itse itseään omavalvonnan ansiosta. Parhaan tuloksen saa, kun rekisteröidyn omat intressit huomioidaan kehittämisessä hyvin. [1]

Sisäänrakennettu ja oletusarvoinen tietosuoja kulkevat siis käsi kädessä: oletusarvoinen tietosuoja on yksi sisäänrakennetun tietosuojan periaatteista ja lopputuloksista. Sisäänrakennetun tietosuojan periaatteet koskevat organisaation kaikkea kehittämistä, ja niiden toteutumista organisaation toiminnassa tulee jatkuvasti kehittää ja arvioida [26]. Sovelluskehityksen yhteydessä sisäänrakennettu tietosuoja tarkoittaa tietojärjestelmiin toteutettavia ominaisuuksia, joiden avulla henkilötietojen käsittelyä voidaan tehdä tietosuoja-asetuksen hengen mukaisesti. Oletusarvoinen tietosuoja taas on velvollisuus huolehtia rekisteröidyn henkilötiedoista ja oikeuksista automaattisesti, ilman, että rekisteröidyn tarvitsee kantaa siitä huolta [3]. Oletusarvoinen tietosuoja sisältää siis lähtöolettaman, että organisaatiot toteuttavat riittävät mekanismit tietosuojan toteutumiseksi [7](25 artikla). Eli: Sisäänrakennetulla tietosuojalla luodaan oletusarvoista tietosuojaa. Tässä tutkielmassa on tarkasteltu nimenomaan sisäänrakennetun tietosuojan vaatimusta.

Rekisterinpitäjällä on velvollisuus varmistaa, että sisäänrakennettu ja sen ohessa myös oletusarvoinen tietosuoja tulevat huomioiduksi tietojärjestelmissä [7](24 artikla). Sisäänrakennettuun tietosuojaan ja sen suunnitteluun on kiinnitettävä huomiota heti, kun sovellusarkkitehtuurin kehittäminen käynnistyy, jotta se saadaan kattamaan koko henkilötiedon elinkaaren [26]. Tärkeää on myös kehittämisen aikana varmistua siitä, että tietosuoja on riittävässä määrin otettu huomioon jokaisessa sovellusarkkitehtuurin ja sovelluskehityksen vaiheessa. Tämä voidaan todentaa katselmointien ja testauksen avulla [30].

Periaatteita ja käytäntöjä, joiden avulla tietosuojavaatimusten implementointia organisaation tietojärjestelmiin voidaan toteuttaa, ovat muun muassa seuraavat [7][29][26]:

- henkilötietojen tallennuksen ja käsittelyn minimointi sekä käsittelyn läpinäkyvyys tarjoamalla rekisteröidylle riittävästi tietoa käsittelystä
- tietojärjestelmien luottamuksellisuuden, eheyden ja käytettävyyden varmistaminen rajoittamalla henkilötietojen käsittelijöiden käyttöoikeuksia sekä huolehtimalla datan laadusta ja tietojärjestelmien turvallisuudesta
- tietojärjestelmien vikasietoisuuden ja palautumiskyvyn varmistaminen sekä turvallisuuden säännöllinen testaaminen ja arvioiminen
- henkilötietojen pseudonymisointi ja anonymisointi sekä salaaminen tietojen siirron ja luovutuksen yhteydessä

- henkilötietoihin pääsyn estäminen rajoittamalla sitä teknisin toimenpitein sekä poistamalla tarpeettomat tiedot
- henkilötietojen käsittelyn lokittaminen: kuka teki ja mitä
- hyvin informoitu suostumus sekä rekisteröidyn omavalvonta: mahdollisuus ja keinot kontrolloida omia henkilötietojaan
- tarkastusmenettelyt tietojen siirtämiseen ja käsittelytarkoituksen laajentamiseen liittyen sekä vaikutustenarviointien laatiminen.

Henkilötietojen **pseudonymisointi** ja **anonymisointi** tarkoittavat henkilötietojen muokkaamista sellaiseen muotoon, ettei tiedoista ole enää joko yksinkertaista tai lainkaan mahdollista selvittää, keneen luonnolliseen henkilöön tieto liittyy. Näitä tiedon tallennuksen periaatteita tulee pyrkiä käyttämään sellaisissa henkilötiedon käsittelytilanteissa, joissa henkilön tunnistaminen ei ole tarpeellista, mutta tieto tapahtumasta halutaan säilyttää esimerkiksi tilastointia varten.

Pseudonymisoidusta henkilötiedosta ei ole mahdollista suoraan nähdä, kenen henkilötiedosta on kyse [7](4 artikla). Tiedon säilyttämisessä on huomioitu se, ettei sen yhteydessä ole muita henkilötietoja, jotka suoraan paljastaisivat rekisteröidyn. Rekisteröidyn henkilön selvittäminen on kuitenkin edelleen mahdollista, jos tietoon liitetään muita toisaalle tallennettuja henkilötietoja. Rekisterinpitäjän tulee pyrkiä toteuttamaan henkilötietojen käsittely niin, ettei tietojen yhdistämistä pääse tapahtumaan eikä rekisteröity näin ollen paljastuisi. Pseudonymisointi vähentää rekisteröityyn kohdistuvia riskejä. Pseudonymisoitua henkilötietoa voidaan siis kuitenkin edelleen käyttää epäsuoraan tunnistamiseen, minkä vuoksi pseudonymisoidut tiedot luokitellaan henkilötiedoiksi. [6]

Anonymisointi puolestaan tarkoittaa henkilötiedoksi luokiteltavien tietojen poistamista muiden tietoalkioiden yhteydestä niin, ettei anonymisoinnin jälkeen ole enää mitenkään mahdollista selvittää, keneen rekisteröityyn henkilöön tiedot ovat liittyneet. Anonymisoitua tietoa voidaan hyödyntää edelleen esimerkiksi tilastointi- tai laskentatarkoituksiin. Kyseisten tietojen ei enää katsota olevan henkilötietoja, joten ne eivät kuulu tietosuojalainsäädännön piiriin. [6]

Sisäänrakennetun tietosuojan tueksi on kehitetty erityisiä tietosuojaa mahdollistavia ja parantavia kaupallisia tai avoimen lähdekoodin teknologiakomponentteja, joita kutsutaan lyhenteellä PETs (Private-Enhancing Technologies). Näihin PETs-komponentteihin luetaan muun muassa tietojen salaamista, anonyymiä kommunikointia, valtuuttamista ja tie-

tokantojen anonyymejä hakuja varten toteutettuja teknisiä ratkaisuja. PETs-komponentit eivät kuitenkaan ole tietoliikenteen salaamiseen tarkoitettuja protokollia lukuun ottamatta muodostuneet suosituiksi, vaan niiden toteuttamisessa on havaittu runsaasti haasteita. Ne eivät myöskään koskaan yksinään riitä toteuttamaan tietosuojaa, vaan niiden lisäksi tarvitaan aina myös tietojärjestelmäkohtaisia sovelluskehityksen ratkaisuja ja organisatorisia käytänteitä, jotta tietosuoja-asetuksen vaatimukset tulevat täytetyiksi. [3]

Sisäänrakennetun tietosuojan periaatteet tulee sisällyttää alusta alkaen myös tietojärjestelmähankintoihin riippumatta siitä, onko hankittava tietojärjestelmä valmisohjelmisto vai toteutetaanko se organisaatiolle räätälöitynä ratkaisuna. Tarjouspyyntöä varten toteutetussa tulevan tietojärjestelmän vaatimusmäärittelyssä tulee jo kuvata järjestelmän tietosuojavaatimukset. Tätä varten organisaatiolla olisi hyvä olla valmiiksi päätettynä ja dokumentoituna sisäänrakennetun tietosuojan toteutusperiaatteet [26]. Mikäli sovelluskehitys ulkoistetaan, voidaan nämä periaatteet liittää tarjouspyyntöön ja hankintasopimukseen ohjaamaan toteutusta. Vaatimusten tulee olla eksakteja ja yksiselitteisesti tulkittavia. Lisäksi tietojärjestelmähankinnan yhteydessä tulee huomioida toimittajan sovelluskehittäjien mahdollinen pääsy organisaation henkilörekistereihin: mikäli sovellustoimittajan työntekijät joutuvat tekemisiin henkilötietojen kanssa, on heitä pidettävä henkilötietojen käsittelijöinä, mikä on huomioitava hankintasopimuksessa. [30]

3.2 Rekisteröitävien henkilötietojen ja oikeusperusteen tunnistaminen

Ennen kuin voidaan päättää tietosuojaan liittyvistä ratkaisuista sovelluskehityksessä, tulee kehittämisen kohteena olevaan toimintoon liittyvät tietoryhmät analysoida ja arvioida, tuleeko kehitettävä tietojärjestelmä sisältämään henkilötietojen käsittelyä. Erikseen on tarve harkita kansallisen henkilötunnisteen eli henkilötunnuksen käsittelytarvetta. Henkilötunnuksesta on tietosuojalaissa todettu, että sitä ei saa käsitellä, ellei käsittelyyn ole saatu rekisteröidyn suostumusta, siitä ole säädetty lailla tai sen käsittely ole tarpeellista rekisteröidyn yksiselitteiksi tunnistamiseksi lakisääteisen tehtävän hoitamiseksi, rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi tai tutkimusta tai tilastointia varten [29]. Lisäksi on todettu, että henkilötunnusta saa käsitellä myös työnantajan velvollisuuksiin liittyvissä tehtävissä ja osoitetietojen päivittämiseksi sekä toiminnassa, johon liittyy taloudellisia riskejä, kuten luotonantoa tai vakuutustoimintaa, tai sosiaali- tai terveydenhuollon palveluita. Henkilötunnusta ei kuitenkaan saa merkitä

asiakirjoihin tarpeettomasti. Näin ollen ensimmäisiksi sisäänrakennetun tietosuojan vaatimuksiksi voi kirjata seuraavat vaatimukset:

> **Vaatimus 1.0**: Rekisterinpitäjän on tunnistettava, käsitelläänkö kehitettävässä tietojärjestelmässä henkilötietoja.
> **Vaatimus 1.1**: Rekisterinpitäjän on tunnistettava rekisteröitävät suorat ja epäsuorat henkilötiedot.
> **Vaatimus 1.2**: Rekisterinpitäjän on varmistettava oikeus tallentaa rekisteröidyn henkilötunnus, jos se tunnistetaan rekisteröitäväksi henkilötiedoksi.
> **Vaatimus 1.3**: Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta käsitellä käyttöliittymässä ilman erityistä tarvetta.
> **Vaatimus 1.4**: Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta merkitä tulosteisiin ilman erityistä tarvetta.
> **Vaatimus 1.5**: Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta luovuteta ilman lakisääteistä oikeutta sen luovuttamiseen.

Tiedonhallintalain pyrkimyksenä on lisätä viranomaisten kesken tapahtuvaa tiedonsiirtoa, jotta rekisteröityjen niin sanottu hallinnollinen taakka eli tarve huolehtia omien tietojensa ilmoittamisesta useille eri viranomaisille vähenisi. Tämä edistäisi myös tietojen oikeellisuutta. Siksi viranomaistoimijan on huomioitava myös mahdollisuus saada henkilötietoja toisilta viranomaisilta. Tästä saamme seuraavan vaatimuksen:

> **Vaatimus 1.6**: Rekisterinpitäjän on pyrittävä hyödyntämään jo kerättyjä henkilötietoja, jos niitä on saatavissa toiselta viranomaiselta.

Mikäli sovelluskehityksen kohteena olevassa tietojärjestelmässä ei käsitellä henkilötietoja eikä näin ollen henkilötietojen rekisteröintiin tule muutoksia, voi organisaatio todeta, etteivät tietosuojaan liittyvät toimenpiteet ole tarpeen. Sen sijaan, mikäli todetaan, että tietojärjestelmään liittyy henkilötietojen käsittelyä, on seuraavaksi selvitettävä kyseisten henkilötietojen käsittelyn lainmukaisuus eli tunnistettava, minkä oikeusperusteen mukaisesti henkilötietoja käsitellään tulevassa tietojärjestelmässä. Oikeusperusteella on vaikutusta muun muassa rekisteröidyn oikeuksiin liittyvien toiminnallisuuksien toteuttamiseen tietojärjestelmässä.

Henkilötietojen käsittelyn lainmukaiset oikeusperusteet ovat seuraavat [7](6 artikla):

- Rekisteröidyn antama suostumus

- Sopimuksen täytäntöön pano
- Rekisterinpitäjän lakisääteinen velvoite
- Rekisteröidyn tai toisen henkilön elintärkeiden etujen suojeleminen
- Rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen
- Rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteutuminen

Oikeusperusteista suurin osa ei itsessään aseta erityisiä vaatimuksia sovelluskehitykselle. Henkilötietoja ei kuitenkaan saa käsitellä lainkaan, ellei sille ole olemassa oikeusperustetta. Siksi oikeusperuste on perustavaa laatua oleva vaatimus myös sovelluskehitykselle. Oikeusperusteet vaativat rekisterinpitäjältä tietynlaista asemaa tai suhdetta rekisteröityyn. Tällaisena suhteena rekisteröidyn ja rekisterinpitäjän välillä voidaan pitää tehtyä tai suunniteltua sopimusta tai asiakas- tai palvelussuhdetta. Näissä tapauksissa on mahdollista, että rekisteröidyn oikeudet ovat voimakkaammat kuin rekisterinpitäjän etu, jolloin rekisterinpitäjän tulee varautua kaikkien rekisteröidyn oikeuksien toteutumiseen tietojärjestelmissä. Toisaalta taas rekisterinpitäjän rekisteröinnin salliva asema voi perustua lakiin kirjattujen velvoitteiden täyttämiseen sekä tämän samoin lakiin kirjattuun oikeuteen suorittaa yleistä etua hyödyttäviä tehtäviä tai käyttää julkista valtaa. Tällöin rekisterinpitäjän velvollisuudet ovat usein vahvempia kuin rekisteröidyn tietyt oikeudet. Henkilötietojen käsittely tilanteessa, jossa käsittelystä on hyötyä rekisteröidyn tai toisen henkilön hengen suojelemiselle, on lisäksi sallittua. Tällainen tilanne voi syntyä humanitaarisista syistä epidemioiden tai katastrofien yhteydessä.

Sen sijaan, jos oikeusperusteena on rekisteröidyn antama suostumus, on tämä huomioitava tietojärjestelmien toteuttamisessa ja rekisteröitävien tietojen määrittelyssä. Tietosuoja-asetuksessa asetetaan suostumukselle tiettyjä vaatimuksia: suostumuksen on oltava rekisteröidyn puolelta vapaaehtoinen, tietoinen ratkaisu, rekisteröintiä varten tehtävän suostumuspyynnön on oltava selkeä ja helposti ymmärrettävä, ja suostumuksen tulee myös olla peruutettavissa yhtä helposti kuin se on annettu ja ilman, että peruutuksesta on haittaa rekisteröidylle [7](7 artikla). Rekisterinpitäjän on kyettävä tarvittaessa näyttämään toteen, että rekisteröity on suostunut rekisteröintiin ja henkilötietojen käsittelyyn. Koska suostumuksen tulee olla selkeästi ja tietoisesti ilmaistu, ei suostumuksena voida pitää tilannetta, jossa henkilö jatkaa tietyllä verkkosivustolla toimimista ilman erityistä suostumuksen ilmaisevaa toimenpidettä, vaikka sivustolla olisikin todettu, että sen käyttäminen

merkitsee henkilötietojen rekisteröintiä ja käsittelyä – tietosuoja-asetuksen sanoin: suostumusta ei pidä voida antaa vaikenemalla. Suostumuksen perusteella rekisteröityjä tietoja ei myöskään saa käsitellä kuin sen antamisen yhteydessä kuvatussa nimenomaisessa käyttötarkoituksessa. Oikeusperusteen tunnistamisesta saamme seuraavan vaatimuksen:

> **Vaatimus 2.1**: Rekisterinpitäjän on tunnistettava lainmukainen peruste henkilötietojen käsittelylle.

Jos henkilötietojen käsittely perustuu rekisteröidyn suostumukseen, silloin vaatimusluetteloon on kirjattava myös seuraavat vaatimukset:

> **Vaatimus 2.2**: Rekisteröidyn on saatava riittävät tiedot henkilötietojen käsittelystä suostumuksen tueksi.
> **Vaatimus 2.3**: Rekisteröidyn on voitava antaa suostumuksensa yksinkertaisella, selkeällä, yksikäsitteisellä tavalla.
> **Vaatimus 2.4**: Rekisterinpitäjän on voitava osoittaa rekisteröidyn tekemä suostumus annetuksi.
> **Vaatimus 2.5**: Rekisterinpitäjän on voitava osoittaa, mihin käyttötarkoitukseen rekisteröity on antanut suostumuksensa.
> **Vaatimus 2.6**: Rekisteröidyn on voitava peruuttaa suostumuksensa yhtä helposti kuin on sen antanut.

Tietosuoja-asetuksessa on mainittu tiettyjä erityistilanteita, joissa henkilötietojen käsittely on lisäksi mahdollista, mikäli näin on säädetty kansallisessa lainsäädännössä. Näitä erityistilanteita ovat muun muassa sanan- ja tiedonvälityksen vapauteen liittyvät tilanteet lähinnä journalistisia ja akateemisia sekä taiteellisen tai kirjallisen ilmaisun tarkoituksia varten. Näitä ei kuitenkaan käsitellä tässä tutkielmassa tämän tarkemmin. [7](85 artikla)

3.2.1 Arkaluonteisten tietojen ja erityisten henkilöryhmien käsittely

Tietojärjestelmässä käsiteltävien henkilötietojen määrittelyn yhteydessä on arvioitava, sisältyykö tietoihin arkaluonteisia henkilötietoja. Näiksi henkilötiedoiksi luetaan sellaiset rekisteröityyn liittyvät tiedot, joiden paljastumisesta voi aiheutua rekisteröidylle suurempaa haittaa kuin muiden henkilötietojen kohdalla. Tällaisten tietojen rekisteröintiä pitää

harkita huolellisesti ja käsittelyä rajoittaa muita tietoja tarkemmin. Näitä arkaluonteisia henkilötietoja ovat seuraavat tiedot [7](8–10 artikla)[22]:

- Alaikäiseen lapseen liittyvät henkilötiedot
- Rekisteröidyn terveydentilaan, biologiaan ja genetiikkaan liittyvät henkilötiedot
- Rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot
- Rekisteröidyn taloudelliseen tilanteeseen liittyvät henkilötiedot kuten ulosotto
- Rekisteröidyn itsemääräämisoikeuteen liittyvät henkilötiedot kuten holhous ja edunvalvonta

Alaikäisten lasten henkilötietojen käsittelyssä on otettava huomioon, ettei rekisteröity lapsi ole välttämättä kykenevä huolehtimaan omien henkilötietojensa suojaamisesta ja rekisteröidyn oikeuksien käyttämisestä riittävissä määrin. Varsinkin tilanteissa, joissa henkilötietoja käytetään suoramarkkinointitarkoituksiin, lapsi luo niillä itselleen henkilö- tai käyttäjäprofiilin tai käyttää suoraan lapsille tarkoitettua palvelua, on rekisteröidyn henkilötietojen suojaamiseen panostettava erityisesti [7](8 artikla). Kansallisen tietosuojalain mukaan suostumukseen perustuva lapsen tietojen rekisteröinti on sallittua, jos tämä on vähintään 13-vuotias [29]. Yhtenä keinona varmistaa alaikäisen lapsen rekisteröinnin sallittavuus on pyytää rekisteröintiin hänen huoltajansa suostumus tai valtuutus käytettävissä olevat tekniset mahdollisuudet huomioiden. Tämä ei kuitenkaan ole soveliasta palveluissa, joiden tarkoituksena on tarjota suoraan lapselle ennalta ehkäiseviä tai neuvontapalveluita kuten lapsille ja nuorille suunnatut ihmissuhteisiin, seksuaalisuuteen ja mielenterveyteen liittyvät palvelut, jotta lapsi ei tarvitsisi vanhemman lupaa saadakseen apua. [7](8 artikla)

Lisäksi tietosuoja-asetuksessa on erikseen mainittu erityiset henkilöryhmät, joiden käsittely on kielletty [7](9 artikla). Näitä erityisiä henkilöryhmiä ovat rotuun ja etniseen alkuperään, poliittisiin mielipiteisiin, uskonnolliseen tai filosofiseen vakaumukseen, ammattiliiton jäsenyyteen tai seksuaaliseen käyttäytymiseen ja suuntautumiseen liittyvät henkilötiedot. Myös geneettisten ja biometristen tietojen käsittely rekisteröidyn tunnistamista varten on kielletty. Rekisteröintikiellosta on mahdollista poiketa vain, jos se perustuu EU:n tai kansalliseen lainsäädäntöön ja on yleisen edun mukaista tai liittyy oikeudelliseen menettelyyn, rekisteröidyn oikeuksien ja elintärkeiden etujen suojaamiseen, rekisterinpitäjän velvoitteiden täyttymiseen, terveys- tai sosiaalihuollon toimintaedellytyksiin,

kansanterveyteen tai jonkin asiaan liittyvän yhteisön kuten puolueen tai ammattiyhdistyksen jäsenyyteen. Lisäksi kyseisiä tietoja on sallittua rekisteröidä, mikäli rekisteröity on erikseen antanut siihen suostumuksensa tai on itse tehnyt kyseiset henkilötiedot julkisiksi. Arkaluonteisten henkilötietojen käsittelyyn pätevät seuraavat vaatimukset:

Vaatimus 3.1: Rekisterinpitäjän on tunnistettava mahdolliset arkaluonteiset rekisteröitävät henkilötiedot.
Vaatimus 3.2: Rekisterinpitäjän on rajoitettava arkaluonteisten henkilötietojen käsittelyä riittävin tietoteknisin ratkaisuin.

Lisäksi, jos rekisteröinti perustuu suostumukseen, on huomioitava seuraavat alle 13-vuotiaan henkilötietojen käsittelyyn liittyvät vaatimukset:

Vaatimus 3.3: Rekisterinpitäjän on suostumuksen antamisen yhteydessä mahdollisuuksien mukaan varmistuttava siitä, että rekisteröitävä on vähintään 13-vuotias
Vaatimus 3.3.1: Rekisterinpitäjän on ilmaistava palvelun ikäraja selkeästi suostumuksen antamisen yhteydessä, jos palvelu ei vaadi vahvaa tunnistautumista.
Vaatimus 3.3.2: Rekisteröitävän huoltajalle on tarjottava ratkaisu suostumuksen tai valtuutuksen antamiseen, jos rekisteröitävä on alle 13-vuotias.
Vaatimus 3.3.3: Lapsen voitava rekisteröityä palveluun ilman huoltajan hyväksymistä, jos kyseessä on lapsille suunnattu ennalta ehkäisevä tai neuvontapalvelu.

3.3 Rekisteröidyn oikeudet

Tietosuoja-asetuksen yksi tärkeimmistä näkökulmista on siihen kirjatut rekisteröidyn henkilön oikeudet omiin henkilötietoihinsa. Kaikkien rekisteröidyn oikeuksien toteutumista on mahdollista ja jopa välttämätöntä tukea tietoteknisillä ratkaisuilla sovelluskehityksen yhteydessä sisäänrakennetun tietosuojan periaatteiden mukaisesti. Rekisteröidyn oikeudet ovat seuraavat [7](12–23 artikla):

- Oikeus saada tiedot henkilötietojen käsittelystä
- Oikeus saada pääsy omiin henkilötietoihin

- Oikeus oikaista virheelliset tiedot
- Oikeus pyytää tiedot poistetuksi (ns. oikeus tulla unohdetuksi)
- Oikeus rajoittaa henkilötietojen käsittelyä
- Oikeus siirrättää omat henkilötiedot toiseen käsittelyjärjestelmään
- Oikeus vastustaa henkilötietojen käsittelyä mm. suoramarkkinointitarkoituksessa
- Oikeus olla joutumatta profiloinnin tai automaattisen päätöksenteon kohteeksi

Ensimmäinen rekisteröidyn oikeuksista koskee hänen oikeuttaan saada informaatiota omien henkilötietojensa käsittelystä. Tämä sama oikeus on sisällytetty myös useaan muuhun rekisteröidyn oikeuteen. Rekisterinpitäjä on velvoitettu pyydettäessä toimittamaan rekisteröidylle tiedot nopeasti, kirjallisesti ja selkeässä ja helposti ymmärrettävässä muodossa. Mikäli pyyntö on tullut sähköisesti, toimitetaan myös tiedot sähköisessä muodossa, ellei rekisteröity ole pyytänyt toisin. Tiedot on toimitettava rekisteröidylle viivytyksittä, normaalitilanteessa kuukauden sisällä pyynnöstä. Mikäli rekisterinpitäjä ei syystä tai toisesta voi toimittaa pyydettyjä tietoja, tulee siitäkin ilmoittaa rekisteröidylle mahdollisimman nopeasti. [7](12 artikla)

Toimitettavien tietojen tietosisältö määräytyy sen mukaan, miten henkilötiedot on saatu. Käytännössä tämä informointivelvollisuus pystytään täyttämään tietosuojaselosteen avulla, jos siihen on kirjattu vaadittavat asiat riittävällä tarkkuudella. Tietosuoja-asetuksessa todetaan, että selosteen käsittelytoimista tulee sisältää vähintään seuraavat tiedot [7](30 artikla):

- rekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot
- henkilörekisterin tietojen käsittelytarkoitus
- rekisteröityjen ryhmät ja henkilötietoryhmät
- tiedonluovutusten saajat
- mikäli tietoja siirretään kolmansiin maihin, tarkemmat tiedot näistä siirroista
- henkilötietojen säilytysajat tietoryhmittäin

- kuvaus teknisistä ja organisatorisista turvatoimista kuten tietojen pseudonymisoinnista ja salaamisesta, järjestelmän luotettavuudesta, vikasietoisuudesta ja palautumiskyvystä sekä tietojenkäsittelyn turvallisuuden testaus- ja arviointimenettelyistä.

Jos henkilötiedot saadaan rekisteröidyltä itseltään, on tietojen saamisen yhteydessä rekisteröidylle ilmoitettava rekisteröitävien henkilötietojen säilytysaika sekä kerrottava hänen oikeuksistaan kyseisiin rekisteröityihin henkilötietoihin. Hänen tulee myös saada rekisteröinnin yhteydessä tietoa henkilötietojen käsittelyn riskeistä, säännöistä ja suojatoimista. Kun hän käyttää oikeuttaan saada informaatiota omien henkilötietojensa käsittelystä, pitää hänelle tietosuojaselosteen vähimmäistietojen lisäksi ilmoittaa henkilötietojen rekisteröinnin oikeusperuste sekä rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, mikäli oikeusperusteena on kyseisten etujen toteutuminen. [7](13 artikla)

Jos taas rekisteröidyt henkilötiedot on saatu muualta kuin suoraan rekisteröidyltä itseltään, on rekisteröityä informoitava saaduista tiedoista joko ensimmäisen yhteydenoton yhteydessä tai kun hänen tietojaan luovutetaan eteenpäin, kuitenkin viimeistään kuukauden sisällä tietojen saamisesta. Tietosuojaselosteen vähimmäistietojen lisäksi rekisteröidylle on tässä yhteydessä ilmoitettava, mitä henkilötietoja (henkilötietoryhmiä) hänestä on rekisteröitynä ja mistä kyseiset henkilötiedot on saatu. Ilmoitusta ei tarvitse tehdä, jos se on mahdotonta tai kohtuuttoman vaivan takana, jos rekisterinpitäjällä on lakisääteinen oikeus saada tai luovuttaa tiedot tai kun tiedot ovat luottamuksellisia. [7](14 artikla)

Kun yllä mainitut lisätiedot lisätään tietosuojaselosteen minimivaatimukseen, kattaa se täysin vaaditun informointivelvoitteen sisällön.

Rekisterinpitäjän on omatoimisesti ilmoitettava rekisteröidylle, mikäli tämän tietoja aiotaan käyttää muuhun tarkoitukseen kuin mihin ne on alun perin kerätty. [7](13 artikla)

Toinen rekisteröidyn oikeuksista koskee hänen pääsyään rekisteröityihin henkilötietoihin. Rekisteröidyllä on oikeus pyytää rekisterinpitäjältä tieto siitä, onko tällä käsiteltävänä hänen henkilötietojaan. Jos näin on, on rekisterinpitäjän tarjottava hänelle pääsy tietoihin joko katselukäyttöliittymän kautta tai toimittamalla hänelle jäljennös kyseisistä henkilötiedoista sekä laajennettu tietosuojaseloste. Tiedot toimitetaan sähköisessä muodossa, jos tietopyyntökin on tullut sähköisenä, ellei rekisteröity itse pyydä tietoja esimerkiksi kirjeitse. [7](15 artikla)

Ensimmäisestä ja toisesta rekisteröidyn oikeudesta voidaan vetää seuraavat vaatimukset sovelluskehitykselle:

Vaatimus 4.1: Rekisteröidyn on saatava määrätyt tiedot henkilötietojensa käsittelystä helposti ymmärrettävässä, selkeässä muodossa.

Vaatimus 4.2: Rekisteröidyn on saatava henkilötiedot antaessaan riittävä tieto rekisteröidyn oikeuksista ja siitä, miten hänen on mahdollista käyttää oikeuksiaan, sekä tietojen säilytysajasta.

Vaatimus 4.3: Rekisteröidyn on voitava antaa tarvittavat tiedot rekisteröintiä varten.

Vaatimus 4.4: Rekisterinpitäjän on voitava tunnistaa, mistä rekisteröidyn henkilötiedot on saatu.

Vaatimus 4.5: Rekisteröidylle on ilmoitettava kuukauden sisällä, jos hänen henkilötietojaan saadaan muualta kuin rekisteröidyltä itseltään.

Vaatimus 4.6: Rekisterinpitäjän on tiedettävä, koska rekisteröity on saanut tiedon henkilötietojensa saamisesta.

Vaatimus 4.7: Rekisteröidyn on saatava tieto siitä, jos kerättyjen henkilötietojen käsittelytarkoitusta laajennetaan.

Vaatimus 4.8: Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä luettavassa, sähköisessä muodossa nopeasti ja luotettavasti.

Kolmas rekisteröidyn oikeus on oikeus tietojen oikaisemiseen [7](16 artikla). Rekisteröidyllä on oikeus vaatia rekisterinpitäjään korjaamaan virheelliset tai epätarkat tiedot mahdollisimman pian ja toimittaa rekisterinpitäjälle lisätietoja korjaamisen tekemiseksi. Rekisteröidyn neljäs oikeus puolestaan koskee oikeutta tietojen poistamiseen eli niin kutsuttua oikeutta tulla unohdetuksi [7](17 artikla). Jos rekisteröity pyytää rekisterinpitäjää poistamaan tiedot itsestään, tulee rekisterinpitäjän poistaa ne viivytyksettä, jos kyseisiä tietoja ei enää tarvita tai rekisteröity on peruuttanut suostumuksen, jonka perusteella henkilötietojen käsittelyä on tehty. Poistamisen perusteena voi myös olla henkilötietojen käsittelyn vastustaminen tai lainvastaisuus tai rekisterinpitäjään sovellettava lakisääteinen velvollisuus. Poistaminen voi olla oikeutettua myös, jos rekisteröity on alaikäinen. Jos henkilötietojen käsittelylle on kuitenkin edelleen olemassa laillinen peruste, ei rekisterinpitäjällä ole velvollisuutta poistaa tietoja. Tietojen poistamista ei tarvitse myöskään tehdä, mikäli niitä tarvitaan sanan- tai tiedonvälityksen vapauden oikeuden perusteella, rekisterinpitäjän lakisääteisen tehtävän vuoksi, kansanterveydellisistä syistä tai yleistä etua palvelevan arkistointitarkoituksen takia. Myös mahdollinen tarve käyttää tietoja oikeudellisissa toimissa on hyväksyttävä syy olla poistamatta niitä.

Viides rekisteröidyn oikeus antaa rekisteröidylle mahdollisuuden rajoittaa henkilötietojensa käsittelyä. Käsittelyn rajoittamisella tarkoitetaan rekisteröidyn henkilötietojen merkitsemistä niin, ettei niitä ole mahdollista käsitellä tietojärjestelmissä enää merkinnän tekemisen jälkeen ilman rekisteröidyn suostumusta [7](4 artikla). Rajoittaminen voi olla oikeutettua, jos henkilötiedot eivät ole paikkansapitäviä, jos käsittely on lainvastaista, jos rekisteröity ei halua tietoja poistettavan, koska tarvitsee niitä oikeustoimia varten, tai jos hän käyttää vastustamisoikeuttaan [7](18 artikla).

Jos rekisteröity on käyttänyt oikeuksistaan oikaisun pyytämistä, tietojen poistamista tai käsittelyn rajoittamista, pitää rekisterinpitäjän ilmoittaa näistä rajoituksista myös kaikille niille, joille kyseisen rekisteröidyn tietoja on luovutettu. Rekisteröidyllä on myös oikeus pyytää tieto siitä, keille hänen tietojansa on luovutettu. [7](19 artikla)

Näistä kolmesta rekisteröidyn oikeudesta saadaan seuraavat vaatimukset vaatimusluetteloon:

Vaatimus 4.9: Rekisteröidyn on voitava ilmoittaa virheellisistä tiedoista tai korjata ne itse.

Vaatimus 4.10: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava korjata virheelliset tiedot.

Vaatimus 4.11: Rekisterinpitäjän on määriteltävä, milloin tietojen poistaminen on mahdollista.

Vaatimus 4.12: Rekisteröidyn on voitava pyytää tietojen poistamista tai poistaa ne itse.

Vaatimus 4.13: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa henkilötiedot tarvittaessa.

Vaatimus 4.14: Rekisteröidyn on voitava vaatia yksilöidysti henkilötietojen käsittelyn rajoittamista.

Vaatimus 4.15: Rekisterinpitäjän on määriteltävä, milloin tietojen käsittelyn rajoittaminen on mahdollista.

Vaatimus 4.16: Rekisterinpitäjän on määriteltävä, minkä henkilötietoryhmien käsittelyä on mahdollista rajoittaa.

Vaatimus 4.17: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä rekisteröidyn tietoihin kyseisten tietojen käsittelyrajoitus.

Vaatimus 4.18: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava ohittaa käsittelyrajoitetut henkilötiedot.

Vaatimus 4.19: Rekisterinpitäjän tai henkilötietojen käsittelijän on pys-

tyttävä tuottamaan tietojärjestelmästä tieto siitä, kenelle tai minne rekisteröidyn tiedot on luovutettu.

Tämän lisäksi on vielä huomioitava seuraava vaatimus, jos henkilötietojen oikaiseminen, poistaminen tai rajoittaminen on aiheellista:

Vaatimus 4.20: Rekisterinpitäjän on voitava toimittaa tietojen oikaisu-, poisto- tai rajoituspyyntö kaikille niille tahoille, joille se on luovuttanut kyseisen rekisteröidyn tiedot.

Rekisteröidyn kuudes oikeus on oikeus siirtää henkilötiedot järjestelmästä toiseen [7](20 artikla). Rekisterinpitäjän tulee voida toimittaa tiedot rekisteröidylle sellaisessa muodossa, jossa ne ovat luettavissa koneellisesti toiseen järjestelmään silloin, kun rekisteröinti perustuu rekisteröidyn antamaan suostumukseen tai sopimukseen tai tietojen käsittelyä suoritetaan automaattisesti. Tämä ei kuitenkaan päde silloin, kun tietojen käsittelyä tehdään yleistä etua koskevan tehtävän tai rekisterinpitäjän julkisen vallan perusteella. Tästä oikeudesta on kiteytettävissä kaksi vaatimusta:

Vaatimus 4.21: Rekisteröidyn on voitava ilmoittaa halustaan siirtää henkilötiedot toiseen tietojärjestelmään.
Vaatimus 4.22: Rekisterinpitäjän on määriteltävä, milloin tietojen siirtäminen tietojärjestelmästä toiseen on mahdollista.

Jos oikeus tietojen siirtämiseen on olemassa, on olemassa myös seuraava vaatimus:

Vaatimus 4.23: Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä sähköisessä, koneellisesti luettavassa muodossa.

Rekisteröidyn seitsemäs ja kahdeksas oikeus koskevat tietojenkäsittelyn vastustamista [7](21 artikla) ja automaattista päätöksentekoa ja profilointia [7](22 artikla). Rekisteröidyllä on oikeus vastustaa henkilötietojen käsittelyä ja automatisoitua päätöksentekoa, jos hänen tietojensa rekisteröinti perustuu yleistä etua koskevan tehtävän suorittamiseen, rekisterinpitäjän julkiseen valtaan tai rekisterinpitäjän tai kolmannen osapuolen etujen toteuttamiseen. Tällöin rekisterinpitäjän pitää keskeyttää rekisteröidyn tietojen käsittely, ellei pysty osoittamaan, että siihen on olemassa riittävät ja perustellut syyt. Jos kyse on

suoramarkkinointi- tai markkina- tai mielipidetutkimustarkoituksessa suoritettavasta henkilötietojen käsittelystä, saa rekisteröity koska vain vastustaa tietojensa käsittelyä. Tästä rekisteröidyn vastustamisoikeudesta on informoitava häntä jo ensimmäisen yhteydenoton yhteydessä (vaatimukset 4.2 ja 4.4). Jos henkilötietoja käytetään suoramarkkinointiin, tulee vastustamisoikeudesta aina ilmoittaa rekisteröidylle. Rekisteröity voi lisäksi kieltäytyä automaattisesta päätöksenteosta ja profiloinnista silloin, jos se vaikuttaa häneen merkittävästi, paitsi jos päätöksenteko tai profilointi on tarpeen sopimuksen tekemistä tai toteutumista varten tai se perustuu rekisteröidyn suostumukseen. Profiloinnilla tarkoitetaan tässä henkilötietojen käsittelyä, jossa rekisteröityä analysoidaan automaattisesti hänestä tallennettujen henkilötietojen perusteella [7](4 artikla). Näistä kahdesta oikeudesta vastustaa henkilötietojen käsittelyä saadaan luetteloon seuraavat vaatimukset:

> **Vaatimus 4.24**: Rekisterinpitäjän on määriteltävä, milloin henkilötietojen käsittelyn vastustaminen tai automaattisen päätöksenteon tai profiloinnin kieltäminen on mahdollista.
> **Vaatimus 4.25**: Rekisteröidyn on voitava vastustaa henkilötietojen käsittelyä tai kieltäytyä automaattisesta päätöksenteosta ja/tai profiloinnista.
> **Vaatimus 4.26**: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä automaattisen päätöksenteon ja profiloinnin kielto rekisteröidyn tietoihin.
> **Vaatimus 4.27**: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava käsitellä manuaalisesti automaattisesta päätöksenteosta estetyt henkilötiedot.

Henkilötietojen käsittelyn vastustamisessa on mahdollista hyödyntää jo aiemmin kirjattua vaatimusta 4.13.

Rekisteröidyn oikeuksia on mahdollista rajoittaa kansallisella lainsäädännöllä tilanteissa, joissa henkilötietojen käsittely liittyy turvallisuuteen, julkiseen etuun, valvonta-, tarkastus- tai sääntelytehtäviin, rekisteröidyn suojeluun tai oikeuskanteiden täytäntöönpanoon. [7](23 artikla)

Sovelluskehityksessä on erityisesti kiinnitettävä huomiota rekisteröidyn oikeuksien toteutumiseen sisäänrakennetun tietosuojan periaatteiden mukaisesti. Varsinkin toisen oikeuden käyttäminen eli rekisteröidyn tietojen toimittaminen rekisteröidylle saattaa kuormittaa rekisterinpitäjää tai henkilötietojen käsittelijää runsain mitoin, ellei henkilötietojen keräämiseen organisaation henkilörekistereistä ole erityisesti kiinnitetty huomiota.

Ennen kuin rekisteröity voi käyttää oikeuksiaan, on rekisterinpitäjän velvollisuutena var-

mistaa, että henkilö, joka haluaa oikeuksia käyttää, on juurikin rekisteröity henkilö. Jos henkilötietojen käsittelyä tehdään sellaisessa tarkoituksessa, jossa rekisteröidyn varma tunnistaminen ei ole välttämätöntä, ei käsiteltävien henkilötietojen tarvitse – eikä niiden edes tulisi – sisältää yksilöllisesti rekisteröidyn identifioivia henkilötietoja kuten henkilötunnusta vain sitä varten, että rekisteröity voitaisiin tunnistaa oikeuksiensa käyttämisen yhteydessä. Rekisterinpitäjä voi esimerkiksi kieltäytyä pyydettyjen tietojen toimittamisesta ainoastaan, jos ei pysty tunnistamaan rekisteröityä. Tällöin rekisterinpitäjä voi kuitenkin pyytää rekisteröidyltä lisätietoja tämän henkilöllisyyden varmistamiseksi. [7](11 artikla)

Tilanteissa, joissa rekisteröity on itse rekisteröitynyt ilman virallista tunnistautumista esimerkiksi sähköpostiosoitteella tai nimimerkillä, ei rekisterinpitäjä voi siis olla täysin varma tämän henkilöllisyydestä. Tällöin rekisteröity joudutaan pyrkimään todentamaan niitä henkilötietoja käyttäen, jotka tämä on itse palveluun antanut. Rekisterinpitäjän tehtävänä on pyrkiä varmistamaan, että rekisteröidyn pyyntö on oikeellinen ja että pyytäjä ja rekisteröity ovat sama henkilö. Jos rekisterinpitäjä ei pysty hallussaan olevien henkilötietojen avulla varmistumaan pyytäjän henkilöllisyydestä, ei tällaisissa tapauksissa voida noudattaa asetuksen vaatimuksia rekisteröidyn oikeuksien täyttämisestä. Tästä voidaan vetää kaksi vaatimusta, joihin tulee löytyä vastaus sovelluskehityksen yhteydessä:

> **Vaatimus 4.28**: Rekisterinpitäjän on määritettävä, miten rekisteröity tunnistetaan niillä tiedoilla, jotka hänestä on olemassa.
> **Vaatimus 4.29**: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava tunnistaa rekisteröity, joka haluaa käyttää rekisteröidyn oikeuksiaan.

3.4 Käsittelyperiaatteet

Henkilötietojen käsittelyperiaatteet, jotka muodostavat tietosuoja-asetuksessa rekisterinpitäjän tietojenkäsittelyyn liittyvien tietosuojavelvollisuuksien ytimen, ovat osittain päällekkäisiä rekisteröidyn oikeuksien kanssa. Käsittelyperiaatteet on lueteltu kappaleessa 2.3. Lyhyemmässä muodossaan ne ovat seuraavat [7](5 artikla):

- Lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate
- Käyttötarkoitussidonnaisuuden periaate
- Tietojen minimoinnin periaate

- Täsmällisyyden periaate
- Säilytyksen rajoittamisen periaate
- Eheyden ja luottamuksellisuuden periaate

Ensimmäinen käsittelyperiaate koskee henkilötietojen käsittelyn laillisuutta, asianmukaisuutta ja läpinäkyvyyttä. Käsittely on lainmukaista, kun se perustuu johonkin asetuksessa mainittuun oikeusperusteeseen, asianmukaista, kun käsittelyä tehdään käsittelyperiaatteiden mukaisesti ja vain tarpeellisilta osin, ja läpinäkyvää, kun rekisteröity saa henkilötietojensa käsittelystä tietoja helposti ja ymmärrettävässä muodossa rekisteröinnin yhteydessä sekä pyydettäessä. Rekisteröidyllä on oikeus saada kysyttäessä vahvistus siihen, käsitelläänkö hänen henkilötietojaan rekisterinpitäjän toimesta, ja tietyissä tilanteissa myös ilmoitus käsittelystä. Rekisteröidylle tulee tarjota mahdollisuus kontrolloida omaa dataansa joko pyynnöstä tai käyttäjäystävällisen sähköisen asioinnin kautta [3].

Toinen periaate on, että tietoja saa kerätä vain tiettyä, erikseen ilmaistua käyttötarkoitusta varten, eikä niitä saa käyttää laajemmassa tarkoituksessa myöhemmin ilman eri harkintaa. Käyttötarkoitus on ilmaistava rekisteröidylle tietojen rekisteröinnin yhteydessä. Kolmas käsittelyperiaate on tietojen minimoinnin periaate: vain sellaisia tietoja saa kerätä, jotka ovat olennaisia ja tarpeellisia niiden käyttötarkoitusta ajatellen. Henkilötietoja ei saa kerätä eikä muuten käsitellä, jos se ei ole välttämätöntä. Neljännessä periaatteessa puolestaan tähdennetään tietojen oikeellisuuden ja täsmällisyyden vaatimusta. Rekisterinpitäjän on mahdollisuuksien mukaan huolehdittava siitä, että rekisteröidyn tiedot ovat ajan tasalla ja että ne voidaan korjata tarvittaessa viipymättä. Jos on olemassa mahdollisuus päivittää tietoja säännöllisesti perusrekisterien avulla, on se suotavaa [3].

Viidennen periaatteen mukaan henkilötietoja tulee säilyttää mahdollisimman lyhyen aikaa niin, että rekisteröidyn voi niistä tunnistaa. Kun tiedot eivät ole enää välttämättömiä säilyttää kerättyyn tarkoitukseensa, tulee ne poistaa tai muuntaa muotoon, josta rekisteröityä ei voi enää tunnistaa. Henkilötiedoille tulee määritellä säilytysajat ja huolehtia niiden poistamisesta säännöllisesti. Kuudes ja viimeinen periaate on eheyden ja luottamuksellisuuden periaate, joka vaatii henkilötietojen suojaamista niin, että ne ovat turvassa asiattomalta käsittelyltä ja tietoturvaloukkauksilta. Käyttöä tulee rajoittaa käyttövaltuuksin [3]. Rekisterinpitäjällä on erikseen määritetty osoitusvelvollisuus sen suhteen, että henkilötietojen käsittelyssä noudatetaan mainittuja periaatteita. [7](5 artikla)

Osa henkilötietojen käsittelyperiaatteista johdettavista vaatimuksista kuten vaatimus lainmukaisesta perusteesta käsittelylle ja rekisteröidyn oikeuksiin liittyvät vaatimukset ovat jo esiintyneet aiemmissa kappaleissa. Uusia vaatimuksia voidaan johtaa varsinkin minimoinnin, täsmällisyyden, säilytyksen rajoittamisen sekä eheyden ja luottamuksellisuuden periaatteista:

> **Vaatimus 5.1**: Rekisterinpitäjän on huomioitava määritetyt käsittelyperiaatteet henkilötietojen käsittelyssään.
> **Vaatimus 5.2**: Rekisterinpitäjän on määritettävä kerättävien tietojen käyttötarkoitus.
> **Vaatimus 5.3**: Rekisterinpitäjän on määritettävä rekisteröitävät tiedot mahdollisimman niukoiksi ja vain määritettyä käsittelytarkoitusta silmällä pitäen.
> **Vaatimus 5.4**: Rekisterinpitäjän on mahdollisuuksien mukaan huolehdittava rekisteröidyn tietojen ajantasaisuudesta tietoteknisin keinoin.
> **Vaatimus 5.5**: Rekisterinpitäjän on määriteltävä henkilötietojen säilytysaika mahdollisimman lyhyeksi.
> **Vaatimus 5.6**: Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa tai anonymisoida henkilötiedot säilytysajan päätyttyä.
> **Vaatimus 5.7**: Rekisterinpitäjän on suojattava henkilötiedot mahdollisimman hyvin asiattomalta pääsyltä.
> **Vaatimus 5.7.1**: Rekisterinpitäjän on suojattava henkilötietojen käsittely soveltuvin käyttövaltuuksin.
> **Vaatimus 5.7.2**: Rekisterinpitäjän on suojattava henkilötietojen käsittelyympäristö soveltuvin teknisin ratkaisuin ja käyttövaltuuksin.

Henkilötietojen säilytysaikaa määritettäessä on huomioitava kansallisessa lainsäädännössä olevat säilytysajat esimerkiksi kirjanpitolakiin tai työnantajan velvoitteisiin liittyen. Kun luodaan poistokäytäntöjä henkilötietojen poistamiseksi säilytysajan jälkeen, on siinä yhteydessä selvitettävä ja käytävä läpi kaikki kyseiseen henkilötietoon liittyvät tallennuspaikat, mukaan lukien mahdolliset välitallennuspaikat sekä varmistusmediat. Rekisterinpitäjän täytyy siis olla hyvin tietoinen siitä, minne henkilötiedot on tallennettu ja minne tietoja on mahdollisesti monistettu. Jokaiselle säilytyspaikalle on määritettävä oma säilytysaikansa. Tästä saadaan seuraavat vaatimukset:

> **Vaatimus 5.8**: Rekisterinpitäjän on varmistettava, että määritelty säilytysaika huomioi erillislainsäädännön.

Vaatimus 5.9: Rekisterinpitäjän on tiedettävä, minne kaikkialle henkilötieto on tallennettu ja monistettu.
Vaatimus 5.10: Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja.

Jos henkilötietojen käyttötarkoitusta halutaan laajentaa alkuperäisestä määrittelystä, pitää uuden käsittelytarkoituksen noudattaa kuitenkin samaa henkilötietojen käsittelyn oikeusperustetta kuin vanha käyttötarkoitus. Jos oikeusperuste muuttuu, ei käyttötarkoitus todennäköisesti ole enää riittävän lähellä alkuperäistä tarkoitusta, jotta sen laajentaminen voitaisiin katsoa sopivaksi. Jos käyttötarkoitusta laajennetaan, on rekisterinpitäjän ilmoitettava tästä ja rekisteröidyn oikeuksista omatoimisesti rekisteröidylle, jos tietojen rekisteröinti perustuu rekisteröidyn suostumukseen tai lainsäädäntöön. [7](6 artikla)

Tietosuoja-asetuksessa on lisäksi erityisiä säännöksiä yleisen edun mukaiseen arkistointitarkoitukseen, tieteelliseen tai historialliseen tutkimustarkoitukseen ja tilastollisen tiedon tuottamiseen liittyvästä henkilötietojen käsittelystä [7](89 artikla). Näissä tapauksissa henkilötietojen käyttötarkoitusta on mahdollista tietyin säännöin laajentaa kuitenkin niin, että huomioidaan erityisesti tietojen minimoinnin periaate: henkilötiedot on mahdollisuuksien mukaan pyrittävä poistamaan tai pseudonymisoinnin avulla huolehtimaan siitä, ettei rekisteröityä ole enää mahdollista kerätystä datasta tunnistaa. Historiallista tutkimusta ajatellen on kuitenkin huomattava, ettei tietosuoja-asetusta sovelleta kuolleiden henkilöiden henkilötietojen käsittelyyn. Erityiset käsittelytarkoitukset huomioidaan seuraavassa vaatimuksessa:

Vaatimus 5.11: Rekisterinpitäjän on huolehdittava henkilötietojen minimoinnista, jos henkilötietoja säilytetään erityisiä käsittelytarkoituksia varten.

3.5 Henkilötietojen siirto ja luovuttaminen

Henkilötietoja voi olla tarvetta siirtää organisaation tai konsernin sisällä, organisaatiolta toiselle, tai luovuttaa kolmansille osapuolille. Siirrettävillä ja luovutettavilla henkilötiedoilla on aina vastaanottaja. Vastaanottaja voi olla rekisteröity, rekisterinpitäjä tai henkilötietojen käsittelijä, mutta myös edellä mainittu kolmas osapuoli, luovutettaviin henkilötietoihin liittymätön ulkopuolinen henkilö tai organisaatio. Viranomaisille

henkilötietoja voidaan luovuttaa niille asetettujen lakisääteisten tehtävien nojalla. Henkilötiedot luovuttavan organisaation on oltava hyvin perillä siitä, millaiset oikeudet sillä on siirtää tai luovuttaa tietoja ja keille, ja henkilötietoja käsittelevän tietojärjestelmän kehittämisen yhteydessä on arvioitava, onko kyseisiä tietoja tarve ja oikeus luovuttaa. Vapaaseen käyttöön henkilötietoja ei koskaan saa altistaa, vaan niiden käyttöä on aina voitava rajoittaa. [7](25 artikla)

Henkilötietojen luovuttamiseksi luetaan myös henkilötietoja sisältävien asiakirjojen antaminen kolmansille osapuolille. Viranomaisilla ja yhteisöillä voi olla laissa säädetty yleisen edun vuoksi suoritettava tehtävä, jonka perusteella niillä on oikeus luovuttaa virallisia asiakirjoja, jotka sisältävät henkilötietoja [7](86 artikla). Tällä eriluvalla mahdollistetaan virallisten asiakirjojen julkisuus. Julkisuuslain mukaan viranomaisrekisterien tiedot ovat pääsääntöisesti julkisia, ja salassa pidettävistä asiakirjoista on erikseen säädetty laissa [19]. Henkilötietojen luovuttamiselle suoramarkkinointiin tai mielipide- ja markkinatutkimuksiin tarvitaan toki aina rekisteröidyn suostumus. Henkilötietojen luovutukseen liittyy seuraavat vaatimukset:

> **Vaatimus 6.1**: Rekisterinpitäjän on varmistuttava henkilötietojen siirron tai luovutuksen lainmukaisuudesta.
> **Vaatimus 6.2**: Rekisterinpitäjän on huolehdittava henkilötietojen näkyvyyden rajoittamisesta soveltuvilta osin.

Jos viranomaisrekisterin tietoja luovutetaan suoramarkkinointiin tai mielipide- tai markkinatutkimuksiin, silloin tulee huomioida myös nämä vaatimukset:

> **Vaatimus 6.3**: Rekisteröidyn on voitava tarvittaessa antaa suostumus tietojen luovuttamiseen suoramarkkinointiin tai mielipide- tai markkinatutkimuksiin.
> **Vaatimus 6.4**: Rekisteröidyn on voitava helposti perua suostumuksensa tietojen luovuttamiseen suoramarkkinointiin tai mielipide- tai markkinatutkimuksiin.

Tiedonhallintalaissa on viranomaiselle asetettu lisäksi useita eri vaatimuksia, jotka liittyvät tietojen siirtoon ja luovuttamiseen ja joiden sisällyttäminen tietojärjestelmiin tulee vaikuttamaan myös henkilötietojen käsittelyyn [17]. Lain yhtenä perusajatuksena on viranomaisten tietoaineistojen hyödyntäminen yli virastorajojen: toisille viranomaisille on tarjottava mahdollisuus käyttää aineistoja joko tiedonsiirtorajapinnan tai tietojärjestelmän katselukäyttöliittymän kautta. Tietoja saadaan luovuttaa, jos vastaanottajalla on siihen

lakiin perustuva oikeus. Luovutusten lainmukaisuudesta ja ylipäätään tarpeellisuudesta tulee kuitenkin varmistua joka kerta, ja tietopyynnöt tulee rekisteröidä viranomaisen asiarekisteriin ja luovutetut tiedot kirjata lokiin. Tiedonhallintalaista voidaan vetää seuraavat vaatimukset, joiden toteuttamisella tuetaan sisäänrakennettua tietosuojaa:

Vaatimus 6.5: Rekisterinpitäjän on toteutettava tietovarantonsa niin, että myös muut viranomaiset voivat niitä hyödyntää.
Vaatimus 6.6: Rekisterinpitäjän on voitava tunnistaa luovutettujen tietojen vastaanottaja.
Vaatimus 6.7: Rekisterinpitäjän on kerättävä lokia tiedonluovutuksista.
Vaatimus 6.8: Rekisterinpitäjän on varmistuttava tiedonluovutuksen tarpeellisuudesta.
Vaatimus 6.9: Rekisterinpitäjän on huolehdittava siitä, ettei käyttöliittymässä ole näkyvissä tarpeettomia tietoja.
Vaatimus 6.10: Rekisterinpitäjän on rekisteröitävä tietopyynnöt asiarekisteriin.

3.5.1 Henkilötietojen siirtäminen kolmansiin maihin

Yhteiskunnan digitalisoituminen ja globalisoituminen ovat tuoneet mukanaan tarpeen siirtää henkilötietoja myös yli valtionrajojen. Koska tietosuoja-asetus koskee vain EU:n jäsenmaita, ei sen avulla voida välttämättä vaatia muita valtioita toteuttamaan EU-kansalaisten tietosuojaa asetuksen vaatimalla tasolla. EU:n on kuitenkin mahdollista säädellä oikeutta siirtää tietoja näihin ulkopuolisiin maihin. Tavoitteena tässä säätelyssä on rekisteröityjen henkilötietojen suojasta ja oikeuksista huolehtiminen.

Henkilötietojen siirtäminen fyysisesti EU:n tai Euroopan talousalue ETA:n ulkopuolelle tai henkilötietojen käsittelytoimenpiteiden suorittaminen mainitun alueen ulkopuolelta käsin on sallittua vain tietyin ehdoin. Tietosuoja-asetuksessa puhutaan tällöin siirrosta kolmanteen maahan tai kansainväliselle järjestölle. Tiedonsiirto voidaan toteuttaa vain, mikäli EU-komissio on erikseen hyväksynyt kolmannen maan tai kansainvälisen järjestön tietosuojakäytännöt riittäviksi [7](45 artikla). Tietoja voidaan mahdollisesti siirtää myös, jos voidaan todeta tietojen vastaanottajan toteuttaneen riittävät toimenpiteet henkilötietojen suojaamiseksi ja rekisteröidyn oikeuksien turvaamiseksi[7](46 artikla). Siirtoon liittyvistä edellytyksistä on erikseen säädetty tietosuoja-asetuksessa. Erikseen on myös todettu ehdot, jonka perusteella monikansalliset yritykset saavat siirtää henkilötietoja konsernin sisällä

kolmansiin maihin [7](47 artikla). Eritystilanteissa henkilötietojen siirto voi olla oikeutettua myös ilman, että kolmas maa täyttää asetetut vaatimukset. Näitä erityistilanteita ovat esimerkiksi rekisteröidyn nimenomainen suostumus siirtoon sekä tietojen siirron tarpeellisuus sopimuksen täytäntöönpanemiseksi tai yleisen edun vuoksi [7](49 artikla). Näissä tiedonsiirtotilanteissa tulee aina tapauskohtaisesti harkita, täyttyvätkö lainmukaiselle tiedonsiirrolle asetetut vaatimukset. Jos tietoja on sallittua siirtää kolmanteen maahan, tulee tämä sekä toteutetut suojatoimet kirjata tietosuojaselosteeseen. Mikäli henkilötietoja siirretään kolmansiin maihin, tulee huomioida seuraavat vaatimukset:

Vaatimus 6.12: Rekisterinpitäjän on varmistuttava henkilötietojen luovuttamisen kolmansiin maihin lainmukaisuudesta.
Vaatimus 6.13: Rekisterinpitäjän on kirjattava arviointi tiedonsiirrosta ja toteutetut suojatoimet tietosuojaselosteeseen.

Hyvänä esimerkkinä EU:n ja kolmannen valtion välisestä sopimuksesta liittyen henkilötietojen siirtoihin on EU:n ja Yhdysvaltojen tekemä Privacy Shield -sopimus [2]. Sen mukaan yhdysvaltalaisten organisaatioiden tulee noudattaa tietosuojavelvoitteita, kun EU-kansalaisten tietoja siirretään ja käsitellään. Sopimuksen perusteella toimivien organisaatioiden tulee myös noudattaa EU:n tietosuojaviranomaisten päätöksiä. Organisaatiot voivat rekisteröityä Privacy Shield -toimijoiksi, ja lista rekisteröityneistä toimijoista on julkisesti saatavilla.

3.6 Henkilötietojen turvallisuuden varmistaminen

Henkilötietojen turvallisuuden varmistaminen on yksi rekisterinpitäjän tärkeimmistä velvollisuuksista. Rekisterinpitäjän tulee tietosuoja-asetuksen mukaan toteuttaa riittävät tekniset ja organisatoriset toimenpiteet suojatakseen henkilörekisterit ylimääräiseltä henkilötietojen käsittelyltä. On niin henkilötietojen käsittelijöiden kuin rekisterinpitäjänkin edun mukaista, että henkilötietojen käsittelyä rajoitetaan vain välttämättömään, työtehtävien mukaiseen tietojenkäsittelyyn. Turvallisuustoimenpiteiden implementoiminen tietojärjestelmiin on sisäänrakennetun tietosuojan periaatteiden mukaista. Toimenpiteiden avulla varmistetaan rekisteröidyn oikeuksien toteutuminen ja täytetään rekisterinpitäjälle asetetut käsittelyperiaatteiden mukaiset velvollisuudet. Tarvittavat toimet tulee mitoittaa sen mukaisesti, miten suuria riskejä henkilötietojen käsittelyyn liittyy. [7](24 artikla)

Organisaation riskienhallintaprosessiin sisällytettävä tietosuojariskien arviointi on yksi keino varmistua henkilötietojen käsittelyn turvallisuudesta ja päättää sitä varten vaadittavista turvallisuustoimenpiteistä. Riskienarvioinnin tavoitteena on varmistaa rekisteröityjen henkilöiden oikeuksien toteutuminen. Tietosuoja-asetuksessa on vaadittu, että rekisterinpitäjä arvioi rekisteröityjen oikeuksiin ja vapauksiin liittyvät riskit, jotka ”voivat aiheutua henkilötietojen käsittelystä, joka voi aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja, erityisesti jos käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, maineen vahingoittumiseen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetykseen, pseudonymisoitumisen luvattomaan kumoutumiseen tai aiheuttaa muuta merkittävää taloudellista tai sosiaalista vahinkoa”. Vaatimus pitää sisällään myös mahdollisen rekisteröidyn oikeuksien menettämisen sekä arkaluonteisen tiedon käsittelystä ja profiloinnista sekä suurista käsittelymääristä johtuvat riskit. Riskienarvioinnissa käydään läpi henkilötietojen käsittelyn luonne ja laajuus, asiayhteys ja käsittelytarkoitukset sekä näistä mahdollisesti löydettävät riskitekijät ja määritetään tarvittavat toimenpiteet, joiden avulla havaittuja riskejä pyritään pienentämään. Arvioinnin yhteydessä on pyrittävä huomioimaan myös mahdolliset henkilötietojen tietoturvaloukkaukset. Riskien todennäköisyyttä ja kriittisyyttä tulee verrata toimenpiteiden toteuttamiskustannuksiin, ja sen perusteella arvioida, mitkä turvallisuustoimenpiteet on järkevää toteuttaa. Riskienarvioinnin tulee kohdistua koko henkilötiedon elinkaareen. [7](32 artikla)

Tyypillisiä tietosuojaa tukevia toimenpiteitä on jo listattu kappaleessa 3.1 liittyen sisäänrakennettuun tietosuojaan. Tietosuoja-asetuksessa riskienarvioinnin perusteella päätettäviksi toimenpiteiksi on nimetty tietojen pseudonymisointi ja salaaminen, käsiteltävien henkilötietojen rajaaminen vain työtehtävien kannalta tarpeellisiin, tietojärjestelmän käytettävyyden ja vikasietoisuuden parantaminen, tietojen eheyden ja luottamuksellisuuden vahvistaminen, palvelun ja tietojen palautumiskyvyn varmistaminen sekä turvallisuustoimenpiteiden säännöllinen arvioiminen [7](32 artikla). Myös henkilötietoja käsittelevän henkilöstön ohjeistaminen henkilötietojen oikeelliseen käsittelyyn on yksi turvallisuustoimenpiteistä [7](28 artikla). Voidaan siis todeta, että samat toimenpiteet tukevat sekä sisäänrakennetun tietosuojan että henkilötietojen käsittelyn tietoturvallisuuden sisällyttämistä tietojärjestelmiin. Tähän liittyviä vaatimuksia ovat:

> **Vaatimus 7.1**: Henkilötietojen käsittelijällä tulee olla oikeudet vain hänen tehtäviensä kannalta tarpeellisiin tietoihin.
>
> **Vaatimus 7.2**: Rekisterinpitäjän on huolehdittava, ettei henkilötietojen käsit-

telijä pääse käsittelemään tarpeettomia henkilötietoja.

Vaatimus 7.3: Rekisterinpitäjän on huolehdittava henkilötietoja käsittelevän tietojärjestelmän riskiarvioinnista ja sen perusteella tehtävistä toimenpiteistä.

Mikäli havaitaan, että henkilötietojen käsittelyn yhteydessä voi rekisteröidyn oikeuksista huolehtimiseen liittyä korkeita riskejä, on rekisterinpitäjän velvollisuutena tehdä vaikutustenarviointi [7](35 artikla). Vaikutustenarvioinnissa arvioidaan riskien alkuperää, luonnetta ja vakavuutta, ja sen lopputuloksena esitetään tarvittavat toimenpiteet, joiden avulla pienennetään havaittua riskiä ja osoitetaan, että henkilötietojen käsittely on lainmukaista. Jos tätä ei voida selvästi osoittaa, joudutaan henkilötietojen käsittelystä ottamaan yhteyttä tietosuojavaltuutettuun. Vaikutustenarviointi tulee tehdä tarvittaessa jo siinä vaiheessa, kun tietojärjestelmän kehittämistä vasta suunnitellaan. Varsinkin silloin, kun henkilötietojen käsittely sisältää automaattista päätöksentekoa tai profilointia, kun käsitellään arkaluonteisia henkilötietoja tai kun tehdään yleisölle avoimen alueen järjestelmällistä valvontaa, on vaikutustenarviointi aiheellista tehdä. Arvioinnissa käydään läpi rekisteröitävät henkilötiedot, niihin liittyvät tietovirrat ja käyttötarkoitukset sekä arvioidaan suunniteltujen käsittelytoimien lainmukaisuutta ja niistä aiheutuvia riskejä. Vaikutustenarviointi liittyy rekisterinpitäjän osoitusvelvollisuuden täyttämiseen. Vaikutuksenarviointia varten kirjataan seuraava vaatimus:

Vaatimus 7.4: Rekisterinpitäjän on huolehdittava vaikutustenarvioinnista, mikäli henkilötietojen käsittelyssä havaitaan mahdollisuus korkeaan riskitasoon.

Myös tiedonhallintalaki ottaa kantaa tietojen ja tietojärjestelmien turvallisuuteen [17]. Sen mukaan tietoturvallisuuden tilaa on seurattava jatkuvasti ja huolehdittava riskienhallinnasta. Tietojärjestelmien vikasietoisuus ja käytettävyys tulee varmistaa testaamalla. Tiedonsiirrot on toteutettava salattua ja suojattua yhteyttä käyttäen ja vastaanottajasta varmistuen. Tietoaineistojen tulee olla virheettömiä ja saavutettavia, ja tietojärjestelmien käyttöä tulee rajata käyttöoikeuksin, joiden pitää olla ajan tasalla. Lisäksi järjestelmien käytöstä ja tiedonluovutuksista tulee kerätä tarpeelliset lokitiedot. Tiedonhallintalaista poimittavat seuraavat vaatimukset vastaavat siis hyvin pitkälle tietosuoja-asetuksen vaatimuksia tai ovat niitä tukevia:

Vaatimus 7.5: Rekisterinpitäjän on toteutettava henkilörekisterinsä vikasietoisiksi ja palautumiskykyisiksi.

Vaatimus 7.6: Rekisterinpitäjän on toteutettava sähköiset tiedonsiirrot salattuja tai suojattuja yhteyksiä käyttäen.
Vaatimus 7.7: Rekisterinpitäjän on huolehdittava, ettei henkilörekistereihin ole oikeuksia kuin heillä, joilla tietojen käsittely kuuluu työtehtäviin.
Vaatimus 7.8: Rekisterinpitäjän on kerättävä lokia tietojärjestelmän käytöstä.

3.6.1 Henkilötietojen tietoturvaloukkaukset

Rekisterinpitäjällä on velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista, mutta niiden tunnistaminen ja löytäminen ei välttämättä ole helppoa. Tietosuoja-asetus määrittelee henkilötietojen tietoturvaloukkauksen seuraavasti: "'henkilötietojen tietoturvaloukkauksella' tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin" [7](4 artikla). Henkilötietojen tietoturvaloukkaus rikkoo eheyden ja luottamuksellisuuden periaatetta, ja siitä on ilmoitettava tietosuojavaltuutetulle 72 tunnin sisällä sen havaitsemisesta, jos rikkomus täyttää ilmoitusvelvollisuudesta säädetyt kriteerit [7](33 artikla). Henkilötietojen tietoturvaloukkaukseksi luetaan siis yllä olevan määritelmän mukainen käsiteltävien tietojen vahingossa tai tahallisesti tapahtuva laiton käsittely, ja se voi johtua teknisestä viasta, inhimillisestä virheestä, varomattomasta toiminnasta tai tahallisesta tietovuodosta. Myös yritys päästä käsiksi tietoon tai jopa fyysiseen tilaan voidaan katsoa tietoturvaloukkaukseksi, jos tätä yrittäneellä henkilöllä ei ole ollut siihen oikeutta [22].

Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi seuraavat tapahtumat [22]:

- Palvelussa on tekninen häiriö, jonka vuoksi henkilötietojen käyttäminen estyy
- Palvelussa on virhe, jonka vuoksi henkilötietoja vuotaa tahoille, joilla ei ole niihin oikeutta
- Henkilötietojen käsittelijä käsittelee (esimerkiksi säilyttää tai katselee) tietoja ohjeiden ja lain vastaisesti
- Henkilötietoja joutuu tietovälineen varkauden tai katoamisen vuoksi vääriin käsiin
- Henkilötietojen käsittelyyn tarvittavia käyttöoikeuksia on levinnyt liian laajalle
- Henkilötietojen käsittelijä luovuttaa henkilötietoja vahingossa väärälle henkilölle

- Postitusvirheen vuoksi henkilötietoja päätyy väärille vastaanottajille
- Ulkopuolinen toimija onnistuu häirinnän, hyökkäyksen tai tietojen kalastelun avulla aiheuttamaan häiriön tai saamaan henkilötietoja käsiinsä.

Tietosuojavaltuutetulle tehtävässä henkilötietojen tietoturvaloukkausilmoituksessa on annettava kuvaus tapahtuneesta loukkauksesta, ilmoitettava loukattujen rekisteröityjen ryhmät ja lukumäärät sekä henkilötietoryhmät ja lukumäärät mikäli mahdollista. Rekisterinpitäjän velvollisuutena on myös dokumentoida henkilötietojen tietoturvaloukkaukset, niiden vaikutukset, tarvittava todistusaineisto ja korjaavat toimenpiteet niin, että sen avulla voidaan tarvittaessa osoittaa, että loukkaukseen on reagoitu tietosuojaa parantamalla [7](33 artikla). Rekisterinpitäjän on myös ilmoitettava tietoturvaloukkauksesta rekisteröidylle itselleen, jos loukkauksesta voi aiheutua tälle haittaa [7](34 artikla).

Henkilötietojen tietoturvaloukkausten havaitsemiseksi ja estämiseksi on huolehdittava seuraavista vaatimuksista:

> **Vaatimus 8.1**: Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin.
> **Vaatimus 8.2**: Rekisterinpitäjän on testattava henkilötietoja käsittelevät järjestelmät sen varmistamiseksi, ettei tietoja vuoda vääriin käsiin.
> **Vaatimus 8.3**: Rekisterinpitäjän on huolehdittava henkilötietojen käsittelyn lokittamisesta, jotta pystytään selvittämään loukatut rekisteröidyt ja henkilötiedot.
> **Vaatimus 8.4**: Rekisterinpitäjän on salattava sen tietovälineille tallennettu data.
> **Vaatimus 8.5**: Rekisterinpitäjän on tarkistettava henkilötietoja sisältävien palveluiden käyttöoikeudet säännöllisesti.
> **Vaatimus 8.6**: Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla henkilötietojen tietoturvaloukkaukset olisi mahdollista havaita.

Tiedonhallintalaki asettaa lisäksi henkilötietojen tietoturvaloukkauksiin liittyen yhden lisävaatimuksen: laissa todetaan, että tietojärjestelmän, jonka kautta toisille viranomaisille tarjotaan mahdollisuus katsella henkilötietoja, olisi tunnistettava mahdolliset poikkeavat haut [17]. Poikkeavien hakujen määrittely kattavasti voi osoittautua vaativaksi tehtäväksi. Tästä on kuitenkin johdettavissa seuraava vaatimus:

Vaatimus 8.7: Rekisterinpitäjän on pyrittävä määrittelemään ja löytämään tietovarantoihin tehtävät poikkeavat haut.

3.7 Osoitusvelvollisuuden täyttäminen

Rekisterinpitäjän osoitusvelvollisuus täytetään riittävän dokumentoinnin avulla. Tietosuoja-asetus vaatii tehtäväksi tietosuojaselosteen kaikista henkilörekistereistä ja niihin liittyvistä henkilötietojen käsittelytoimista [7](30 artikla). Selosteen sisältö on kuvattu kappaleessa 3.3. Tietosuojaseloste vaaditaan myös kaikilta rekisterinpitäjän lukuun henkilötietojen käsittelyä tekeviltä. Selosteen tulisi olla nähtävillä palvelussa, jossa siinä mainitun henkilörekisterin tietoja käsitellään tai jossa rekisteröity henkilö luovuttaa tietojaan rekisterinpitäjälle. Rekisteröidyn tulee lisäksi saada tietosuojaseloste nähtäväkseen pyydettäessä. Rekisterinpitäjän velvollisuutena on pitää tietosuojaselosteen tiedot ajan tasalla. Sovelluskehityksen yhteydessä on täytettävä seuraavat vaatimukset:

Vaatimus 9.1: Rekisterinpitäjän on liitettävä tietosuojaseloste rekisteröidyille tarjottaviin palveluihin näiden nähtäväksi.
Vaatimus 9.2: Rekisterinpitäjän on huolehdittava tietosuojaselosteen ajantasaisuudesta.

Kappaleessa 3.6 esitellyt riskienarviointi ja vaikutustenarviointi ovat myös omalta osaltaan osoitusvelvollisuuden mukaista dokumentaatiota.

Julkishallintoa koskevat tiedonhallintalain vaatimukset tukevat erittäin hyvin tietosuoja-asetuksen osoitusvelvollisuutta [17]. Vaatimus prosessien ja tietovarantojen kuvaamisesta sisältää myös henkilötietojen käsittelyprosessit ja henkilötietoja sisältävät tietovarannot fyysisine sijainteineen sekä niiden väliset tietovirrat. Vaadituista kuvauksista syntyy tiedonhallintamalli-niminen dokumentaatio, jossa henkilötietojen käsittelyyn liittyviä kuvauksia tulee olemaan muun muassa prosesseihin, tietovarantoihin ja niiden sisältämiin tietoryhmiin, tiedonluovutuksiin, tietojen säilytysaikaan, tietoaineiston arkistointiin, tietojärjestelmiin ja tietoturvallisuustoimenpiteisiin liittyen. Tiedonhallintamallin tulee olla julkishallinnon organisaatioissa kuvattuna 1.1.2021 mennessä. Jos rekisterinpitäjä on viranomainen, koskevat sitä tiedonhallintalaista poimittavat seuraavat vaatimukset:

Vaatimus 9.3: Rekisterinpitäjän on dokumentoitava rekisteröidyt henkilötiedot ja niiden käsittelijät.

Vaatimus 9.4: Rekisterinpitäjän on kuvattava henkilötietovirrat rekistereittäin sisältäen tietolähteet, tietoja käyttävät tietojärjestelmät, henkilötietojen siirrot järjestelmien välillä ja henkilötietojen käsittelyn fyysiset sijainnit.
Vaatimus 9.5: Rekisterinpitäjän on dokumentoitava tiedonluovutukset ja siirrot kolmansille osapuolille sekä niiden perusteet.
Vaatimus 9.6: Rekisterinpitäjän on kuvattava henkilötietojen säilytysajat ja poistomekanismit.
Vaatimus 9.7: Rekisterinpitäjän on kuvattava tietoturvallisuustoimenpiteet, joiden avulla henkilörekisterien turvallisuus on toteutettu.

Tiedonhallintamallin tuottaminen rekisterinpitäjän osoitusvelvollisuuden tueksi vähintään henkilötietoja käsittelevistä prosesseista, tietovarannoista ja tietojärjestelmistä olisi suositeltavaa muidenkin kuin viranomaisten osalta.

Tietojärjestelmien käytön ja henkilötietojen käsittelyn lokittaminen toimii myös osoitusvelvollisuuden täyttäjänä. Lokien avulla voidaan tarvittaessa käyttää niin käsittelyperiaatteiden noudattamisen kuin rekisteröityjen oikeuksien toteutumisen valvontaan kuin myös epäiltyjen henkilötietojen tietoturvaloukkausten selvittämiseen [17].

Organisaatio voi osoittaa toimivansa tietosuoja-asetuksen velvoitteiden mukaisesti sertifioitumalla EU:n hyväksymän sertifiointimekanismin käyttöön [7](25 artikla). Olemassa olevista sertifiointimekanismeista on saatavissa tieto Euroopan tietosuojaneuvoston sivuilta [10].

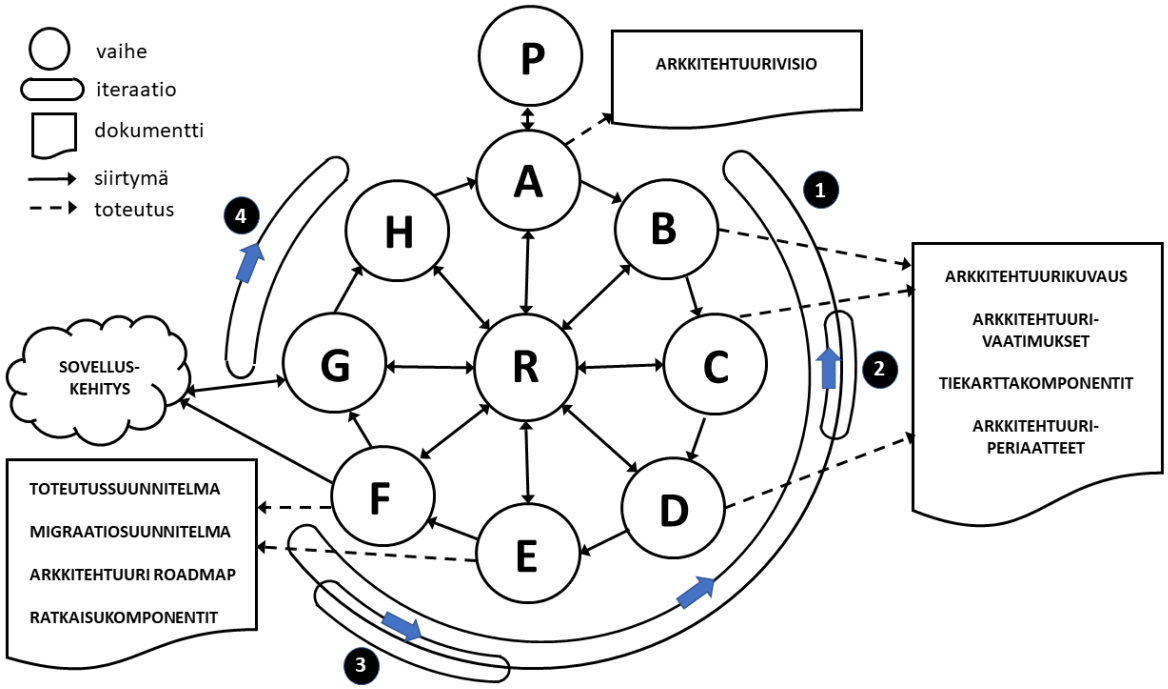
4 Sisäänrakennetun tietosuojan huomiointi sovelluskehityksessä

Edellisessä kappaleessa esiteltiin EU:n yleisestä tietosuoja-asetuksesta [7] sekä kansallisen lainsäädännön tietosuojalaista [29], julkisuuslaista [19] ja tiedonhallintalaista [17] löydetyt sisäänrakennetun tietosuojan vaatimukset. Kyseiset vaatimukset tulee huomioida sovelluskehityksen yhteydessä, kun kehitetään henkilötietoja käsitteleviä tietojärjestelmiä ja niihin liittyviä henkilörekistereitä. Jotta tämä osataan tehdä oikea-aikaisesti, on vaatimukset hyvä järjestää loogiseen aikajärjestykseen ja kiinnittää sovelluskehitystä tukevaan arkkitehtuurikehykseen. Tutkielmassa on käytetty viitekehyksenä yhtä maailman tunnetuimista kokonaisarkkitehtuuriviitekehyksistä eli Open Groupin TOGAF-mallia (The Open Group Architecture Framework) ja sen versiota 9.1 [24].

Tämän kappaleen aluksi esitellään lyhyesti TOGAF-mallin sisältämä arkkitehtuurin kehittämisprosessi ja sen jälkeen liitetään sisäänrakennetun tietosuojan vaatimukset sen vaiheisiin.

4.1 TOGAF: Arkkitehtuurin kehittämisprosessi

TOGAF 9.1 -kokonaisarkkitehtuuriviitekehys [24] sisältää useita ohjekokonaisuuksia, jotka tukevat organisaation kokonaisarkkitehtuurin (enterprise architecture) kehittämistä. TOGAFin ytimen muodostaa arkkitehtuurikehittämisen prosessimalli ADM (Architecture Development Method). ADM rakentuu kymmenestä vaiheesta, jotka yhdessä muodostavat iteratiivisesti etenevän arkkitehtuurin kehittämisprosessin. ADM on tarkoitettu nimenomaan kokonaisarkkitehtuurin kehittämiseen, mutta iteratiivisen ja syklisen luonteensa vuoksi se on käyttökelpoinen kehys myös pienemmässä mittakaavassa tapahtuvalle sovelluskehittämiselle. Malli itsessään on myös iteratiivinen: TOGAFin mukaan ADM-mallia voidaan käyttää strategisen arkkitehtuuritason luomiseen, joka käynnistää puolestaan segmenttiarkkitehtuurin tai tiettyä kyvykkyyttä varten toteutettavan arkkitehtuurin ADM-prosessin. Toisin sanoen ADM:n avulla luodaan ensin karkeamman tason arkkitehtuurikuvaus, jota myöhemmillä kehityskierroksilla täsmennetään ja yksityiskohtaistetaan. Näin ollen se sopii käytettäväksi myös tilanteessa, jossa tavoitteena on toteuttaa uusi



Kuva 4.1: TOGAF ADM-kehittämisprosessi
[24]

tietojärjestelmä tai uusi versio jo olemassa olevasta tietojärjestelmästä. Valmis kokonaisarkkitehtuurikuvaus syntyy monien ADM-iteraatioiden kautta.

Kuvassa 4.1 on esitetty ADM-kehittämisprosessin vaiheet, niiden väliset siirtymät tai yhteydet, prosessiin kuvatut iteraatiokierrokset sekä tärkeimmät eri vaiheissa tuotettavasta dokumentaatiosta [24]. ADM-kehittämisprosessin vaiheet ovat seuraavat:

P. Alustus (Preliminary)

A. Arkkitehtuurivisio (Architecture Vision)

B. Toiminta-arkkitehtuuri (Business Architecture)

C. Tietojärjestelmäarkkitehtuuri (Information Systems Architecture)

D. Teknologia-arkkitehtuuri (Technology Architecture)

E. Mahdollisuudet ja ratkaisut (Opportunities and Solutions)

F. Siirtymäsuunnittelu (Migration Planning)

G. Toteutuksen hallinta (Implementation Governance)

H. Arkkitehtuurin hallinta (Architecture Change Management)

R. Vaatimustenhallinta (Requirements Management)

P. Alustus -vaihe tehdään organisaatiossa käytännössä vain kerran. Vaihe antaa pohjan kaikelle organisaation arkkitehtuurityölle: sen tavoitteena on rakentaa organisaatiolle arkkitehtuurikyvykkyys eli arkkitehtuurikehittämisen rakenteet kuten arkkitehtuurityön ohjausprosessi, sen resurssit ja arkkitehtuurityön periaatteet, joiden avulla organisaatiolla on jatkossa riittävä osaaminen tehdä arkkitehtuurityötä muissa ADM:n vaiheissa.

A. Arkkitehtuurivisio -vaihe aloittaa varsinaisen arkkitehtuurin kehittämissyklin. Sen tavoitteena on muodostaa korkean tason visio siitä, mitä alkavalla kehittämishankkeella tavoitellaan. Vaiheen aikana määritellään konkreettinen ongelma, jota ollaan ratkaisemassa, luodaan yhteinen kuva kehittämisen lopputuloksesta, määritellään kehittämistyön sidosryhmät, asetetaan tavoitteet kehittämiselle ja päätetään työn rajaukset. Vaiheen lopputuotoksena on dokumentti, jossa on kuvattu kehittämistyön arkkitehtuuriperiaatteet ja visio lopputuloksesta. Vaihetta voi verrata perinteisen projektinhallintaprosessin suunnitteluvaiheeseen, jossa luodaan pohja projektille ja asetetaan tarvittavat tavoitteet ja reunaehdot ohjaamaan sen läpivientiä.

Kokonaisarkkitehtuurimallit sisältävät tyypillisesti kolme tai neljä eri arkkitehtuurikerrosta. TOGAF jakaa arkkitehtuurikerrokset (liike)toiminta-, tietojärjestelmä- ja teknologia-arkkitehtuureihin. Tietojärjestelmäarkkitehtuuri puolestaan jaetaan tieto- ja sovellusarkkitehtuureihin. Seuraavissa vaiheissa **B. Toiminta-arkkitehtuuri, C. Tietojärjestelmäarkkitehtuuri** ja **D. Teknologia-arkkitehtuuri** suunnitellaan näiden arkkitehtuurikerrosten arkkitehtuuri vaiheessa A luodun vision tueksi ja ratkaistaan se, minkälaiset vaikutukset käynnistyneellä kehittämishankkeella on nykyarkkitehtuuriin. Vaiheet ovat keskenään tehtäviltään ja lopputuotoksiltaan muuten saman sisältöisiä, mutta ne keskittyvät eri arkkitehtuurikerroksiin. Vaiheita suoritetaan iteratiivisesti, jolloin arkkitehtuurikuvausta täsmennetään askel askeleelta muissa vaiheissa tehtyjen suunnitelmien pohjalta. Kussakin vaiheessa valitaan kehittämisessä käytettävät mallit ja välineet, ja luodaan kuva arkkitehtuurin nykytilasta (baseline architecture) sekä ensimmäinen versio tavoitearkkitehtuurista (target architecture). Yksi vaiheessa käytettävistä menetelmistä on kuiluanalyysi (GAP analysis), jossa arkkitehtuurin nykytilaa verrataan tavoitearkkitehtuuriin ja arvioidaan, millä keinoin ja askelin nykytilasta päästään siirtymään tavoitetilaan. Tässä yhteydessä kuvataan mahdolliset arkkitehtuurikomponenttikandidaatit toteutusta varten. Nämä komponenttikandidaatit ovat tässä vaiheessa vielä niin kutsuttuja

arkkitehtuurisia rakennuskomponentteja (architectural building blocks, ABB, myöhemmin arkkitehtuurikomponentit) eli abstrakteja arkkitehtuurin osia, joista tavoitearkkitehtuuria lähdetään kokoamaan. Kokonaisarkkitehtuuriajattelun mukaista on pyrkiä hyödyntämään ja uusiokäyttämään jo olemassa olevia komponentteja ja resursseja. Lisäksi tunnistetaan ja kuvataan uusia komponentteja, joita tarvitaan tavoitteen toteuttamiseksi. Vaiheen lopuksi järjestetään sidosryhmäkatselmointi, jonka jälkeen vielä viimeistellään vaiheen lopputuotokset eli tavoitearkkitehtuurimäärittelyt ja -vaatimukset (architecture definition document ja architecture requirements document), ensimmäiset hahmotelmat tavoitteeseen johtavista tiekartoista (architecture roadmap components) sekä A-vaiheen tuotosten pohjalta täsmennetyt arkkitehtuuri- ja liiketoimintaperiaatteet.

E. Mahdollisuudet ja ratkaisut -vaiheessa luodaan kehittämishankkeen tiekartta ja tarvittavat transitioarkkitehtuurit edellisten vaiheiden lopputuotosten pohjalta. Transitioarkkitehtuurilla tarkoitetaan siirtymää, välivaihetta matkalla kohti varsinaista tavoitearkkitehtuuria. Transitioarkkitehtuurin ideana on toteuttaa kokonaismuutos osissa niin, että kustakin transitiovaiheesta saadaan jo ulosmitattua todellisia hyötyjä ja lisäarvoa organisaatiolle, vaikka ne ovatkin vasta askeleita tavoitearkkitehtuurin suuntaan. Tässä vaiheessa yhdistetään vaiheiden B, C ja D osa-arkkitehtuurikuvaukset yhdeksi kokonaisarkkitehtuurikuvaukseksi ja luodaan kokonaiskuva kuiluanalyyseissa havaituista toimenpiteistä ja kehittämistarpeista, joita tarvitaan, jotta päästään tavoitteeseen. Nämä transitiovaiheen ”askeleet” yhdistetään sopiviksi työpaketeiksi (work package), jotka sisältävät loogisesti yhteenkuuluvia muutoksia, jotka on tarvetta toteuttaa samanaikaisesti. Työpaketit järjestetään ja aikataulutetaan tiekarttaan ja jaetaan mahdollisesti useammaksi transitiovaiheiksi. Vaiheessa päätetään myös tulevat ratkaisun rakennuskomponentit (solution building blocks, SBB, myöhemmin ratkaisukomponentit), jotka ovat täsmällisiä, konkreettisia ja nimettyjä arkkitehtuurin osia, joiden avulla toteutetaan edellisissä vaiheissa määritellyt abstraktit arkkitehtuurikomponentit. Vaiheen lopputuotoksena on siis alustava versio varsinaisesta toteutussuunnitelmasta (implementation and migration plan): tiekartta, työpaketit ja ratkaisukomponentit.

B–E-vaiheissa kuvattavat arkkitehtuurilliset ja ratkaisun rakennuskomponentit (building blocks) ovat sovelluskehityksessä tarvittavia tai syntyviä komponentteja, arkkitehtuurin osia, jotka toteuttavat tietyn toiminnallisen kokonaisuuden. Hyvä rakennuskomponentti on hyvin kuvattu, uudelleenkäytettävä ja tarvittaessa helposti korvattavissa toisella rakennuskomponentilla. Ne on ideaalisesti ajateltuna toteutettu helposti käyttöönotettaviksi, koska niihin on rakennettu valmiit rajapinnat tai muut yhteydet, joiden avulla niitä on

kohtuullisen helppo hyödyntää osana sovellusarkkitehtuuria. Yksi rakennuskomponentti voi koostua useammasta pienemmästä rakennuskomponentista, ja yksi rakennuskomponentti voi kuulua useaan isompaan rakennuskomponenttiin. Arkkitehtuurikomponentit ovat vielä loogisella tasolla olevia kuvaavia komponentteja, joille on määritelty niiden sisältämät ominaisuudet. Ratkaisukomponentit ovat puolestaan valmiita tai tulevia arkkitehtuurikomponenttien toteutuksia. Ne voivat olla esimerkiksi uudelleenkäytettäviä sovellusosia, spesifiin tarkoitukseen tehtyjä sovelluskomponentteja tai myös valmisohjelmistoja, jotka sisällytetään toteutukseen. Yksi esimerkki arkkitehtuurikomponentista on tietokanta, jonka ratkaisukomponentteja ovat eri tietokantatuotteet. TOGAFin määrittelyn mukaan ”arkkitehtuuri on tietty joukko rakennuskomponentteja, jotka on kuvattu tietyllä arkkitehtuurimallilla, ja määrittelyt siitä, miten nuo rakennuskomponentit on yhdistetty, jotta ne täyttävät liiketoiminnan vaatimukset”. Rakennuskomponenteista voidaan myös muodostaa valmiita arkkitehtuurimalleja (architecture pattern), jotka esittävät jo hyväksi todetun loogisen ratkaisun tiettyyn mahdollisesti toistuvaan tarpeeseen.

F. Siirtymäsuunnittelu -vaiheessa suunnitellaan vaiheen E työpaketeista muodostettavat projektit eli tehdään varsinaiset toteutussuunnitelmat, joissa kussakin toteutetaan yhden tai useamman työpaketin sisältämät muutokset. Vaihe F:ssä tehtävät suunnitelmat voivat vaikuttaa E-vaiheen lopputuloksiin, joten näiden kahden vaiheen välillä suoritetaan iterointia. Vaiheen lopputuotoksena on viimeistelty tiekartta ja sen toteuttavien projektien projektisuunnitelmat. Tämä on viimeinen varsinainen arkkitehtuurisuunnitteluvaihe ADM-mallissa: suunniteltua arkkitehtuurivisiota ei saa enää muuttaa tämän vaiheen jälkeen ilman, että muutokset tehdään muutospyyntöinä arkkitehtuurin muutoshallinnan eli H-vaiheen kautta.

Varsinainen arkkitehtuurimuutosten toteutus tietojärjestelmiin eli sovelluskehitysprojektien läpivienti ei kuulu TOGAF-malliin, vaan toteutusprojekti viedään läpi erikseen valittavan ohjelmistotuotantomallin mukaisesti. Tässä tutkielmassa toteutusprojektiin viitataan termillä **sovelluskehitysvaihe**. Sovelluskehitysvaihe on tyypillisesti projekti, jonka projektisuunnitelma tehtiin F-vaiheessa. Valittujen ratkaisukomponenttien toteutuksen yhteydessä on hyvin mahdollista, että joitakin uusia ratkaisukomponenttitarpeita havaitaan vasta tässä vaiheessa. Tällainen tilanne voi tulla eteen esimerkiksi silloin, kun muutoksen kohteena oleva alkuperäinen tietojärjestelmäarkkitehtuuri on iältään ja teknologialtaan vanhentunutta, jolloin sovelluskehitysvaiheessa sen tilalle löydetäänkin uusia, parempia toteutusvaihtoehtoja.

Täysin irti ADM:stä ei kuitenkaan sovelluskehitysvaihekaan ole. ADM:n vaiheen **G.**

Toteutuksen hallinta tehtävänä on valvoa, että varsinainen tietojärjestelmätoteutus tehdään vaiheissa A–F tehtyjen suunnitelmien mukaisesti, ja vaihetta suoritetaankin rinnakkain sovelluskehitysvaiheen kanssa sen kanssa aktiivisesti kommunikoiden. Vaihe G sisältää valvontapisteitä, joissa suunnitelmanmukaisuudesta varmistutaan. Jos poikkeamia havaitaan, on olemassa kolme etenemisvaihtoehtoa: annetaan lupa poiketa suunnitellusta, muutetaan arkkitehtuurisuunnitelmia tai vaaditaan korjaamaan toteutus arkkitehtuurisuunnitelmien mukaiseksi. Näistä vaihtoehdoista kaksi ensin mainittua vaihtoehtoa viedään käsiteltäväksi seuraavaan vaiheeseen H.

Vaiheen **H. Arkkitehtuurin hallinta** englanninkielinen nimi on harhaanjohtava. Sen lisäksi, että vaiheessa tehdään varsinaista arkkitehtuurin muutoksenhallintaa, hoidetaan siinä myös koko arkkitehtuurityön valvontaa (governance). Vaiheessa viimeistellään uudet arkkitehtuuridokumentit ja päivitetään olemassa olevat dokumentit vastaamaan uutta nykytilaa. Muutoksenhallinnassa otetaan kantaa tehtyihin muutospyyntöihin. Päätetyt muutokset voidaan luokitella pieniin muutoksiin, jotka aiheuttavat arkkitehtuurin päivityksen, poikkeuslupiin, jotka eivät varsinaisesti muuta kokonaisarkkitehtuuria, mutta jotka perustelluista syistä hyväksytään, ja suuriin muutoksiin, jotka vaativat koko ADM-syklin uudelleenkäynnistämistä. Mahdolliset vaiheessa G tehdyt havainnot tarpeesta muuttaa suunniteltua arkkitehtuuria aiheuttavat usein vaiheessa H päätöksen uudesta arkkitehtuurisuunnittelukierroksesta. Tässä vaiheessa tarkastellaan myös sitä, tehdäänkö arkkitehtuurin kehittämisessä oikeita asioita, saavutetaanko niistä toivottuja hyötyjä ja noudatetaanko prosessissa organisaatiossa sovittuja käytäntöjä kuten esimerkiksi katselmointeja. Kun toimintaympäristö muuttuu, arvioidaan vaiheessa myös näiden muutosten mahdollista vaikutusta arkkitehtuuriin. Onkin mahdollista, että arkkitehtuurin kehittämissykli käynnistyy johtuen tässä vaiheessa tehdyistä itsenäisistä havainnoista toimintaympäristöön liittyen. Muutosajurina voi toimia niin liiketoimintamuutos kuin teknologiamuutostarvekin.

Kuten todettu, on ADM-malli iteratiivinen. Kuvassa 4.1 on ADM-prosessiin merkitty neljä eri iteraatiokierrosta eri vaiheiden välille:

1. Vaiheiden A–F välillä on ADM-syklin pisin iteraatiokierros nimeltään arkkitehtuurikehityksen iteraatio (Architecture Development Iteration). Mikäli myöhemmissä vaiheissa tehtävät ratkaisut vaativat aiempien vaiheiden tulosten muuttamista tai tarkentamista, on se näin ollen mahdollista. Iteraation avulla pystytään huolehtimaan arkkitehtuurin kokonaiskuvasta.

2. Vaihe C on itsessään iteroiva johtuen vaiheen jakautumisesta tieto- ja sovellusarkki-

tehtuureihin, joissa tehtävät ratkaisut voivat vaikuttaa toisiinsa.

3. Vaiheet E ja F muodostavat transitiosuunnittelun iteraatiokierroksen (Transition Planning Iteration), joka tukee tiekartan suunnittelua. Vaiheessa F tehtävät valinnat voivat tarkentaa tai muuttaa myös vaiheen E kuvauksia.

4. Vaiheet G ja H muodostavat arkkitehtuurinhallinnan iteraation (Architecture Governance Iteration), jossa vaiheessa G havaitut arkkitehtuuripoikkeamat voivat muokata vaiheen H kuvauksia ja vaiheessa H tehdyt päätökset vaiheen G tuloksia. Tämän iteraation avulla tuetaan muutoksenhallintaa.

Kaikkien näiden prosessina kulkevien vaiheiden keskellä ADM-mallissa on **R. Vaatimustenhallinta** -vaihe. Tämän vaiheen tehtävänä on pitää kirjaa arkkitehtuurin kehittämisprosessissa esiintyvistä vaatimuksista. Tämä vaatimustenhallintavaihe on itse asiassa oma hallinnollinen prosessinsa, joka on rinnakkainen arkkitehtuurin kehittämisprosessille. Vaatimuksia voi syntyä missä tahansa ADM-mallin vaiheessa, ja niitä voidaan vastaavasti hyödyntää kaikissa vaiheissa. Vaatimustenhallintavaihe ei priorisoi vaatimuksia eikä tee suunnitelmia niiden toteuttamiseksi, vaan se toimii vain niiden kirjaajana.

Arkkitehtuurikuvaukset ja mahdolliset referenssidokumentit tallennetaan arkkitehtuurirepositorioon. Repositorioon dokumentoidaan voimassaolevat arkkitehtuurit (Architecture Landscape), mallidokumentit kuten sopimuspohjat, arkkitehtuurityössä käytettävät menetelmät, viitekehykset ja standardit, tehdyt arkkitehtuuripäätökset (päätösten audit trail -loki), käytettävät ratkaisuarkkitehtuurikomponentit ja -tuotteet (Solution Landscape) sekä tulevat arkkitehtuurivaatimukset (Requirement Repository). TOGAFiin kuuluu myös sisältömalli (Content Framework), jossa on kuvattu kaikki eri ADM-vaiheissa tuotettavat lopputuotokset (deliverable), toteutetut dokumentit (artifacts) ja rakennuskomponentit. [24]

4.2 Vaatimusten kiinnittäminen arkkitehtuurikehittämisen vaiheisiin

Kappaleessa 3 kerätyt vaatimukset ovat listattuna liitteessä A. Kyseiseen liitteeseen on lisäksi merkitty, missä ADM-mallin vaiheissa niihin on kiinnitettävä huomiota. Tässä kappaleessa on kuvattu ne ADM-prosessin vaiheet, joihin sisäänrakennetun tietosuojan

vaatimuksia ensisijaisesti liitetään. Kukin vaatimus voi lisäksi tulla käsittelyyn myös muissa vaiheissa. Tässä kappaleessa vaiheisiin viitataan joko edellisessä kappaleessa pääsääntöisesti vaiheiden kirjaintunnuksilla (4.1). Sovelluskehitykseen suoraan vaikuttavat sisäänrakennetun tietosuojan arkkitehtuurivaatimukset käsitellään vaiheissa B, C ja D, joiden lopputuotoksena syntyvää arkkitehtuuridokumentaatiota vielä täsmennetään ja tarkennetaan vaiheissa E ja F. TOGAFin mukaan vaiheissa syntyy seuraavat dokumentit [24]:

- Arkkitehtuurimäärittelyyn yhdistetään vaiheiden tulokset eli eri arkkitehtuurikerrosten määrittelyt nykytilan, tavoitetilan ja transitiovaiheen osalta: kehittämiskohteen kuvaus, tavoitteet ja rajaukset, arkkitehtuuriperiaatteet, nykytilan arkkitehtuurikuvaus, käytettävät arkkitehtuurimallit, kuiluanalyysi ja transitioarkkitehtuurit
- Arkkitehtuurivaatimukset on arkkitehtuurimäärittelyn rinnakkaisdokumentti: arkkitehtuurin toiminnalliset vaatimukset ja niiden mittarit, mahdolliset palvelusopimukset, toteutusohjeita ja -määrittelyjä, toteutuksessa käytettävät standardit, yhteentoimivuusvaatimukset, palvelunhallintavaatimukset sekä rajoitteet ja olettamukset
- Arkkitehtuuritiekartta aikatauluttaa toteutuksen: työpaketit, niiden tavoitteet, lopputulokset, toiminnalliset vaatimukset, riippuvuudet ja liiketoiminnalle tuottama lisäarvo, transitioarkkitehtuurit sekä toteutussuositukset ja ratkaisukomponentit.

Vaiheessa E ja F sekä sovelluskehitysvaiheessa huomioitavien vaatimusten osalta on sisäänrakennettuun tietosuojaan vaikuttavat ratkaisut pääsääntöisesti tehty jo aiemmissa vaiheissa, minkä vuoksi vaiheita ei käsitellä tässä sen tarkemmin. Poikkeuksena tähän on kaksi vaatimusta, jotka tulevat huomioitavaksi vasta sovelluskehitysvaiheessa: vaatimukset liittyen tietoturvatestaukseen ja normaalista poikkeavien hakujen havaitsemiseen tulee ottaa tehtävälistalle käynnistyvissä sovelluskehitysprojekteissa arkkitehtuurimäärittelyistä tulevien vaatimusten lisäksi.

Vaiheissa A, G ja H huomioitavat vaatimukset ovat pääosin kehittämistyön perusteisiin ja organisatoristen toimenpiteiden toteuttamiseen liittyviä vaatimuksia. Koska vaihe A antaa tarvittavat rajaukset sisäänrakennetun tietosuojan tasolle, on se käsitelty seuraavassa kappaleessa yhdessä vaiheen B kanssa. Vaiheessa G tulee kiinnittää huomiota sovelluskehitysvaiheen aikaiseen tietosuojaan eli henkilötietojen käsittelyyn projektin aikana, sekä jatkaa riskienarviointia. Vaiheen H vaatimukset liittyvät puolestaan dokumentointiin eli osoitusvelvollisuuden täyttämiseen: rekisterinpitäjän on huolehdittava arkkitehtuuridoku-

menttien päivittämisestä, tietosuojaselosteen tekemisestä ja ajantasaistamisesta sekä tiedonhallintamalliin liittyvän dokumentaation toteutuksesta. Näitä vaatimuksia ei käsitellä tässä sen enempää.

4.2.1 Henkilötietojen käsittelyn lähtökohdat ja toiminta-arkkitehtuuri

Kun suunnitellaan sovellusarkkitehtuurin kehittämistä tai pienempimuotoisempaa sovelluskehitystä, tulee jo sitä suunniteltaessa käydä läpi erinäisiä vaatimuksia, jotka vaativat organisatorisia toimenpiteitä. Tämä tehdään vaiheessa A. Arkkitehtuurivisio. Usein organisaatiolla on olemassa malli, jolla kehittämistoimenpiteet – hankkeet, projektit ja muut kehittämistehtävät – käynnistetään. Myös tietosuojaan liittyvät perusvaatimukset tulisi huomioida tässä mallissa. Mikäli vaiheessa todetaan, ettei henkilötietoja käsitellä kehittämisen kohteena olevassa tietojärjestelmässä, voidaan kaikki muut tietosuojavaatimukset jättää huomiotta. Jos sen sijaan todetaan, että kehitettävä sovellus tai tietojärjestelmä käsittelee henkilötietoja, tulee loput vaatimukset ottaa huomioon. Vaiheen A vaatimukset tuottavat pohjatietoa ja rajauksia seuraaville vaiheille.

Arkkitehtuurivisio-vaiheessa selvitetään, millä perusteella henkilötietoja käsitellään ja minkälaisia rekisteröidyn oikeuksia tietojen suhteen on oikeutettua käyttää, sekä päätetään henkilötietojen käyttötarkoituksesta. Lisäksi arvioidaan vision pohjalta havaittavat riskit. Jos havaitaan, että suunniteltuun toimintaan sisältyy suuria tietosuojariskejä, on rekisterinpitäjän velvollisuutena käynnistää vaikutustenarvioinnin tekeminen, jotta sen päätösten vaikutukset kyetään huomioimaan jo ennen varsinaisen arkkitehtuurisuunnittelun käynnistymistä.

Vastuu vaiheen tehtävistä voi vaihdella: riippuen organisaatiosta ja kehittämisen kohteesta vaihe voi olla substanssin tai tietohallinnon johdon taikka esimerkiksi projektitoimiston vastuulla. Joka tapauksessa tässä vaiheessa luodaan perusta henkilötietojen käsittelyn periaatteille kyseisessä kehittämistehtävässä.

Pääosa vaiheessa A käsiteltävistä tietosuojavaatimuksista tulee käsiteltäväksi myös vaiheissa B ja H. Lisäksi tässä vaiheessa käynnistettävää riskienarviointia jatketaan myöhemmissä vaiheissa.

Yhteenveto Arkkitehtuurivisio-vaiheen tehtävistä:

- Henkilötietojen käsittelyn oikeusperusteen ja käsittelytarkoituksen selvittäminen

- Rekisteröidyn oikeuksien määrittely
- Riskienarvioinnin käynnistäminen
- Mahdollinen vaikutustenarviointi

Toiminta-arkkitehtuurikerroksen kehittämisvaiheen B aikana tuotetaan toiminnalliset vaatimukset kehitettävälle tietojärjestelmälle [24]. Henkilötietojen käsittelyyn liittyen vaiheessa B suunnitellaan prosessit, joiden avulla rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet toteutuvat. Organisaation on muun muassa päätettävä, miten rekisteröity voi käyttää rekisteröidyn oikeuksiaan, miten tämä tunnistetaan oikeuksien käyttämisen yhteydessä ja miten rekisteröidylle tuotetaan sekä rekisteröidyn oikeuksien että ilmoitusvelvollisuuden perusteella toimitettavat tiedot oikea-aikaisesti. Rekisteröidyn oikeuksiin liittyvät vaatimukset ovat riippuvaisia siitä, miten oikeudet on oikeusperusteen ja tietojen käyttötarkoituksen perusteella vaiheessa A määritetty. Tiedonluovutukseen liittyvien prosessien osalta on määriteltävä, minkälaisia tiedonluovutuksia kolmansille osapuolille on oikeus tehdä ja mitä toimenpiteitä luovutukset esimerkiksi sopimusteknisesti vaativat. Tiedonluovutusten perusteet on kuvattava ja sovittava säännöt niiden tekemiselle. Myös henkilötietoja sisältävien asiakirjojen luovuttaminen kolmansille osapuolille on tiedonluovutusta. Näiden osalta on jo tässä vaiheessa varmistettava, että tiedonluovutus on lainmukaista. Ja toisinpäin: mikäli rekisterinpitäjä on viranomainen, on tämän varmistettava, että julkisuuslain mukaiset tiedonluovutukset toteutetaan, vaikka asiakirjat sisältävätkin henkilötiedoiksi luokiteltavia tietoja.

Rekisteröidyn velvollisuuksien käyttämiseen ja rekisterinpitäjän ilmoitusvelvollisuuteen liittyvät vaatimukset voivat olla manuaaliprosesseja, jotka tulee kuvata tai vähintään varmistaa, että organisaatiolla on olemassa riittävät prosessit rekisteröidyn oikeuksista huolehtimiseksi ja että kyseisiä prosesseja voidaan käyttää myös nyt kehittämisen kohteena olevissa toiminnoissa. Lisäksi viranomaisorganisaatiossa on otettava jo tässä vaiheessa selvitykseen mahdollisuus hyödyntää jonkun muun viranomaisen keräämiä henkilötietoja.

Yksi tärkeä vähintään alustavasti päätettävä seikka on henkilötietojen säilytysaika. Kaikille henkilötiedoille tulee päättää säilytysajat, joissa huomioidaan mahdolliset erillislakien vaatimukset sekä organisaation edun mukaiset tarpeet, mutta kuitenkin niin, että tietoja ei säilytetä varmuuden vuoksi kuin korkeintaan lyhyen aikaa esimerkiksi häiriötilanteiden selvittelyn varalta. Organisaation tulee myös määrittää, keillä on oikeus käsitellä mitäkin henkilötietoja. Mikäli henkilötietojen käsittelyssä tullaan käyttämään ulkopuolisia tiedonkäsittelijöitä, tulee sen osalta kirjata tarvittavat toimenpiteet esimer-

kiksi sopimuskäsittelyyn liittyen. Riippuen henkilötietojen käsittelijöiden tehtävistä voi tällä olla vaikutuksia käyttövaltuussuunnitteluun.

Vaiheen lopputulosten kuvaustyyli riippuu kehitettävästä kohteesta ja organisaation käyttämistä kuvausmalleista. Tulokset voidaan kuvata esimerkiksi käyttäen arvoketjuja ja niihin liittyviä kyvykkyyksiä tai organisaatiokarttaa, jossa kyvykkyydet on liitetty organisatorisiin yksiköihin tai merkitty tuotettavaksi ulkoisten palveluntuottajien toimesta. Toimintojen kuvaamisessa voidaan käyttää erilaisia toimintomallien kuvausmenetelmiä kuten prosessikuvauksia tai aktiviteettikaavioita, käyttötapauskuvauksia ja luokkakaavioita. Kuvauksiin sisällytetään arkkitehtuurikomponenteiksi prosesseja, liiketoimintasääntöjä ja työkuvauksia, joita organisaatiossa on jo olemassa, sekä tunnistetaan uusia tarvittavia arkkitehtuurikomponentteja, jotka tulee toteuttaa kehittämisprosessin aikana. [24]

Vaiheen lopuksi jatketaan riskienarviointia katselmoimalla sen lopputuotoksia, jotka toimivat lähtömateriaalina muiden arkkitehtuurikerrosten suunnittelulle. Toiminta-arkkitehtuurivaiheessa tarvitaan näkemystä organisaation toiminnasta ja sen kehittämisestä. Siksi vaiheen tehtävät ovat tyypillisesti substanssiasiantuntijoiden ja arkkitehtien vastuulla.

Yhteenveto B. Toiminta-arkkitehtuuri -vaiheen sisäänrakennettuun tietosuojaan liittyvistä tehtävistä:

- Henkilötietojen käsittelyprosessien kuvaaminen
- Mahdollisten tiedonluovutusten määrittely
- Säilytysaikojen päättäminen
- Riskienarvioinnin jatkaminen

4.2.2 Tietoarkkitehtuurin kehittäminen

Vaiheessa C suunnitellaan sekä tieto- että sovellusarkkitehtuureihin kehitystyön yhteydessä tehtävät muutokset [24]. Vaiheeseen liitetyt vaatimukset voidaan jakaa näiden arkkitehtuurikerrosten mukaan. Monessa tapauksessa vaatimuksella on vaikutusta sekä tietoarkkitehtuurin että sovellusarkkitehtuurin kehittämiseen. Tämän vuoksi vaihe C. Tietojärjestelmäarkkitehtuuri jaetaankin tässä tutkielmassa tästä eteenpäin kahdeksi rinnakkaiseksi vaiheeksi: **C1. Tietoarkkitehtuuri** (C. Information Systems Architecture, data architecture) ja **C2. Sovellusarkkitehtuuri** (C. Information Systems Architecture, application architecture).

Tietosuoja-asetuksesta ja muusta lainsäädännöstä kerätyt tietoarkkitehtuurivaatimukset liittyvät rekisteröitävien henkilötietojen ja henkilötietoryhmien tunnistamiseen. Lisäksi vaatimuksena on rekisteröidä tietoja, joiden avulla kyetään toteuttamaan rekisteröidyn oikeudet: suostumus rekisteröintiin tai tiedonluovutukseen, suostumukseen liittyvä käyttötarkoitus, henkilötietojen alkuperä sekä käsittelyn rajoittamiseen liittyvät merkinnät. Mikäli rekisteröidyn tietoja luovutetaan kolmansille osapuolille, tulee tästä jäädä tieto rekisterinpitäjälle. Jos henkilötiedot on saatu tiedonluovutuksena toiselta rekisterinpitäjältä, tulee luovutusajankohdasta olla olemassa tieto, jotta vaatimus rekisteröidylle ilmoittamisesta voidaan suorittaa määrätyn ajan sisällä. Samoin tulee rekisteröidä tieto siitä, koska tämä ilmoittaminen on suoritettu. Myös mahdollisuus merkitä tiedot poistetuiksi on tyypillisesti tarpeen. Erityisesti on huomattava, että suostumuksen peruuttamisen tulee tarkoittaa myös henkilötietojen poistamista kyseisestä palvelusta.

Tietoarkkitehtuurissa on huomioitava henkilötietojen minimoinnin vaatimus: mitään sellaista henkilötietoa ei ole sopivaa käsitellä, mitä ei nimenomaisesti tarvita määritellyssä käsittelytarpeessa. Henkilötiedoista on myös tunnistettava suorat ja epäsuorat henkilötiedot ja pyrittävä mahdollisuuksien mukaan eriyttämään näitä niin, ettei epäsuoran, pseudonymisoidun henkilötiedon avulla olisi helposti selvitettävissä, keneen luonnolliseen henkilöön tiedot liittyvät. Tämä vaatii harkintaa esimerkiksi rekisteröidystä käytettävän tunnisteen osalta: henkilötunnuksen käyttö primääriavaimena tietokannassa ei ole suotavaa missään tilanteessa, samoin sähköpostiosoitteen käyttöä avainnuksessa tulisi välttää. Rekisteröidyn tietojen avainnukseen ja yhdistämiseen rekisterinpitäjän eri henkilörekistereiden välillä tulee mieluummin käyttää erillistä tunnistetietoa, joka ei yksinään paljasta rekisteröityä. Tunnisteena voidaan käyttää surrogaattiavainta tai erillistä nimettyä tunnistetta kuten asiakasnumeroa, jos arvioidaan, että sitä tullaan tarvitsemaan myös tietojen hakemiseen käyttöliittymässä. Surrogaattiavaimen ja erillisen tunnisteen käyttö yhdessä voi myös olla järkevää riippuen toteutettavasta ratkaisusta ja käytettävästä teknologiasta.

Rekisteröidyn oikeuksien käyttämisen yhteydessä tulee rekisteröity tunnistaa riittävän varmasti. Tätä varten on rekisteröidystä oltava riittävät, vaikkakaan ei käyttötarpeeseen nähden liian kattavat tiedot olemassa. Toisaalta on myös huomioitava tiedot, joiden avulla rekisteröidyn tulee mahdollisesti voida tunnistautua palveluun. Tarvittavat tunnistautumistiedot riippuvat organisaation valitsemasta tunnistautumismetodista.

Mikäli rekisterinpitäjä on viranomainen, tulee tietoarkkitehtuuria määritettäessä huomioida toiselta viranomaiselta saatavien tietojen tallentaminen tietokantaan niin, että niiden

päivittäminen toisen viranomaisen järjestelmästä on yksinkertaista. Samoin on syytä arvioida tietokantarakennetta siitä näkökulmasta, onko tietojen luovuttaminen toiselle viranomaiselle tarvittaessa toteutettavissa helposti. Samassa yhteydessä on hyvä kuitenkin ottaa huomioon myös mahdollisuus siihen, että toiselta rekisterinpitäjältä saatavat henkilötiedot ovat virheellisiä. Tämän vuoksi on hyvä olla olemassa myös suunnitelma siihen, miten tiedot sellaisessa tapauksessa voidaan oikaista.

Tietoarkkitehtuurin suunnittelussa on sisäänrakennetun tietosuojan vaatimusten osalta muun muassa määriteltävä, mihin tietovarantoon on tallennettu rekisteröidyn henkilön tietojen niin sanotut perustiedot (master data). Saman tiedon erillistä ylläpitoa useampaan tietokantaan tulisi aina välttää, koska tiedon eheyttä ei voida silloin taata. Siksi ylläpito tulisi aina kohdistaa vain perustietoon, josta sitä hyödynnetään rajapintojen kautta tai tarvittaessa monistetaan muihin tietokantoihin. Henkilötietojen säilytyspaikat tulee kuvata ja säilytysrakenteet ratkaista myös ajatellen tietojen poistamista: tietokannan viite-eheyksissä on huomioitava mahdolliset tulevat henkilötietojen fyysiset poistot ja pseudonymisoinnit.

Tietoarkkitehtuurin suunnitteluun vaikuttaa lisäksi se, miten liiketoimintaprosessit hyödyntävät tietoa. Henkilötietojen luominen, säilyttäminen, siirtäminen eri tietokantojen ja tietojärjestelmien välillä sekä muuntaminen eri tietojärjestelmien käyttöön soveltuvaksi tulee kuvata. Vaiheen aikana on myös suunniteltava, miten mahdollisesti jo olemassa oleva data migroidaan tarvittaessa uuteen kantaan. Kokonaisarkkitehtuuriperiaatteiden mukaisesti tulisi tietoarkkitehtuurissa huomioida jo olemassa olevien tietoarkkitehtuurikomponenttien hyödyntäminen kehittämisessä.

Arkkitehtuurimäärittelykuvauksessa tulee vaiheen jälkeen olla henkilötiedoista kuvattuna vähintään tarvittavat henkilötietoryhmät ja käytettävät tietovarannot eli henkilörekisterit, henkilötietojen käsittelysäännöt sekä tietovirrat eri henkilörekisterien välillä. Kuvausmallit ovat organisaatioriippuvaisia: käsitemallit, UML-luokkakaaviot, ER-diagrammit ja tietovirta- eli DFD-kaaviot (data flow diagram) ovat käyttökelpoisia kuvausmalleja tässä vaiheessa. [24]

Yhteenveto C1. Tietoarkkitehtuuri -vaiheen sisäänrakennettuun tietosuojaan liittyvistä tehtävistä:

- Rekisteröitävien henkilötietojen tunnistaminen
- Rekisteröidyn oikeuksien täyttämiseen liittyvien tietojen tunnistaminen
- Henkilötietojen avainnuksen määrittely

- Toisen rekisterinpitäjän tietojen hyödyntämisen ratkaiseminen
- Henkilötietojen tallennuspaikkojen ja poiston vaatimien ratkaisujen määrittely
- Mahdollisen datamigraation huomioiminen

4.2.3 Sovellusarkkitehtuurin kehittäminen

Kappaleessa 3 kerätyistä sisäänrakennetun tietosuojan vaatimuksista noin puolella on vaikutuksia sovellusarkkitehtuuriin. Vaatimukset on tässä jaoteltu

- rekisteröidyille tarkoitettuihin sähköisiin palveluihin vaikuttaviin vaatimuksiin
- käyttövaltuuksiin liittyviin vaatimuksiin
- henkilötietojen käsittelijän käyttämään sovellukseen vaikuttaviin vaatimuksiin
- tiedonluovutuksiin ja tiedon vastaanottoon liittyviin vaatimuksiin ja
- henkilötietojen poistamiseen liittyviin vaatimuksiin.

Rekisteröidyille tarkoitetuissa sähköisissä palveluissa, jotka käsittelevät rekisteröidyn henkilötietoja, on huomioitava tämän oikeus saada riittävä informaatio rekisteröitävistä tiedoista, niiden käsittelystä, riskeistä ja suojatoimista sekä rekisteröidyn oikeuksista kyseisiin tietoihin ja oikeuksien käyttämisestä. Näiden tietojen informointiin voi käyttää tietosuojaselostetta, joka sisältää pääosan vaadituista tiedoista, liittämällä se palvelun yhteyteen niin, että rekisteröity voi siihen halutessaan tutustua. Samaan yhteyteen tulee liittää selostukset myös niistä ilmoitusvelvollisuuden piiriin kuuluvista yllämainituista seikoista, joita ei välttämättä ole tietosuojaselosteeseen kirjattu. Mikäli palveluun rekisteröitymisen oikeusperusteena on rekisteröidyn suostumus, on se pyydettävä rekisteröityvältä henkilöltä niin, että voidaan katsoa hänen varmasti tienneen rekisteröitymisestään: suostumus on tietoista, kun se vaatii rekisteröidyn tietoisia toimia kuten suostumusluvan rastittamisen ja valinnan hyväksymisen. Jos rekisteröidyn tietoja käytetään viranomaisen toimesta suoramarkkinointi- tai mielipide- tai markkinatutkimustarkoituksiin, tulee tähänkin pyytää erillinen suostumus. Rekisteröidylle tulee myös kertoa mahdollisuudesta peruuttaa suostumus. Peruuttamisen pitää onnistua yhtä helposti kuin suostumuksen antaminen. Suostumuksen peruuttamisen tulee myös poistaa rekisteröidyn tiedot henkilörekisteristä, ellei ole olemassa muuta oikeusperustetta, jonka perusteella tiedot saa

edelleen säilyttää. Suostumukseen liittyvässä rekisteröinnissä on huolehdittava mahdollisuuksien mukaan siitä, että rekisteröity on vähintään 13-vuotias. Vähimmäisvaatimuksena on palvelun ikärajan kertominen selkeästi suostumuksen antamisen yhteydessä. Joissain palveluissa voi olla tarpeellista pyytää huoltajan suostumusta. Poikkeuksena ovat lapsille ja nuorille tarkoitetut ennalta ehkäisevät ja neuvontapalvelut, joiden käyttöä ei saa estää ikärajalla tai huoltajalta vaadittavalla suostumuksella. Rekisteröinnin yhteydessä tulee rekisteröityvältä pyytää vain niitä henkilötietoja, jotka ovat välttämättömiä palvelun käyttämiseksi. Palvelun yhteydessä on hyvä myös informoida, miten rekisteröity voi korjauttaa virheelliset tiedot tai poistattaa tietonsa, jos rekisteröinti perustu oikeusperusteeseen, jonka vuoksi rekisteröidyllä on oikeus pyytää tietojensa poistamista. Varsinkin sellaisissa palveluissa, joissa rekisteröitävät henkilötiedot saadaan vain rekisteröidyltä itseltään, on mahdollista antaa rekisteröidylle itselleen oikeus korjata tai poistaa tiedot. Mikäli palvelu ei vaadi rekisteröidyn identifiointia, vaan perustuu rekisteröidyn itsensä valitsemaan käyttäjätunnukseen tai ilmoitettuun sähköpostiosoitteeseen, rekisteröity voi antaa palveluun myös vääriä henkilötietoja. Tällöin rekisteröidyn oikeuksien käyttäminen voidaan jättää rekisteröidyn itsensä huolehdittavaksi eli toteuttaa palveluun toiminnallisuudet, joiden avulla hän voi itse katsella tietojaan, muuttaa niitä ja poistaa ne.

Organisaation sovellusarkkitehtuuriin on syytä sisällyttää rakennuskomponentit, jotka toteuttavat rekisteröidyn informointiin, suostumuksen antamiseen ja peruuttamiseen, oikeuksien käyttämiseen ja tunnistautumiseen liittyvät vaatimukset yhtenevästi kaikkiin sähköisiin palveluihin. Samoin tämän tyyppisissä palveluissa tulee olla yhteiset tietoturvaperiaatteet, joiden avulla varmistutaan siitä, ettei palveluiden kautta ole mahdollista aiheuttaa henkilötietojen tietoturvaloukkausta esimerkiksi sql-injektiota käyttäen, ja että palvelussa tehtävät poikkeavat haut tai kirjautumiset voidaan havaita. Rekisteröityjen käyttämien palveluiden käyttöä tulee lokittaa tallentamalla lokiin sekä onnistuneet että epäonnistuneet kirjautumiset kuin myös palvelussa tehtävät muutokset henkilötietoihin.

Henkilötietoja käsittelevän tietojärjestelmän käyttövaltuuksiin liittyen on tietosuoja-asetuksessa muutama vaatimus. Henkilötiedot on suojattava asiattomalta pääsyltä, ja kunkin käsittelijän on voitava käsitellä vain niitä henkilötietoja, jotka ovat tarpeellisia hänen työtehtäväänsä nähden. Toisin sanoen henkilötietojen käsittely tulee suojata käyttövaltuuksin niin, ettei kenellä tahansa organisaatiossa ole mahdollisuutta niitä käsitellä. Henkilötietojen käsittelysovelluksen toimintojen käyttöä tulisi tarvittaessa rajoittaa käyttövaltuuksin luomalla käyttövaltuusryhmiä eli käyttäjärooleja, joilla annetaan oikeudet vain niihin sovelluksen toimintoihin, joita kyseiseen käyttövaltuusryhmään

kuuluvilla henkilötietojen käsittelijöillä on tarvetta työtehtäviensä nojalla käyttää. Käyttövaltuuksin pystytään näin erottamaan toisistaan esimerkiksi henkilötiedon katselijat ja ylläpitäjät. Käyttöoikeusryhmissä on syytä huomioida myös mahdolliset ulkoiset henkilötietojen käsittelijät. Rekisterinpitäjällä on velvollisuus myös pitää lokia tietojärjestelmään kirjautumisista ja uloskirjauksista niin onnistuneiden kuin epäonnistuneiden yritysten osalta. Tietojärjestelmän sovellusarkkitehtuurista riippuen voi olla myös syytä lokittaa järjestelmän käyttäjän liikkuminen sen eri osissa. Lokien avulla on mahdollista havaita henkilötietojen tietoturvaloukkauksia. Mainitut vaatimukset edellyttävät organisaatiolta käyttövaltuuksiin, käyttäjän tunnistamiseen ja lokitietoihin liittyviä toteutusperiaatteita, jotta arkkitehtuurin toteutus olisi hallittua ja koordinoitua. Yhtenä toimintona käyttövaltuuksia hallinnoivassa sovelluksessa tulisi lisäksi olla käyttövaltuuksien hallintaa tukeva mahdollisuus tuottaa käyttövaltuudet sähköisessä muodossa tarkastettavaksi, jotta ylimääräiset käyttövaltuudet saadaan karsittua pois käytöstä.

Henkilötietojen käsittelijän käyttämän sovelluksen käyttöliittymäsuunnittelussa tulee huomioida eri käyttäjärooleille annettavat oikeudet henkilötietojen käsittelyyn. Yhtenä sisäänrakennetun tietosuojan vaatimuksena on, että henkilötietojen käsittelijät saavat käsitellä vain tarpeellisia tietoja. Tämä täytyy huomioida käyttäjärooleja ja käyttötapauksia määriteltäessä. Tiedot on suotavaa ryhmitellä käyttöliittymään käyttötapausten mukaan, jolloin on mahdollista välttää liiallisen tiedon esittämistä käsittelijälle. Tämä koskee varsinkin arkaluonteisia henkilötietoja, joiden osalta käsittelijöiden määrää tulee erityisesti rajata. Samoin henkilötietojen ylläpitämisen mahdollistavat toiminnot tulee rajata vain tarpeelliselle joukolle käyttäjiä. Ylläpitooikeudet omaavalla henkilötietojen käsittelijällä tulee tarvittaessa olla mahdollisuus korjata ja poistaa henkilötietoja. Lisäksi, mikäli rekisteröidyllä on oikeus rajoittaa hänestä rekisteröityjen tietojen käsittelyä, tulee käsittelijällä olla mahdollisuus sekä merkitä henkilötiedot, joiden käsittelyä rajoitetaan, että tapauskohtaisesti ohittaa kyseisten tietojen käsittely. Jos tietojärjestelmässä tehdään automaattista päätöksentekoa, tulee käsittelijällä sen lisäksi olla mahdollisuus tehdä päätös tarvittaessa manuaalisesti. Myös tässä sovelluksessa on huomioitava henkilötietojen käsittelyn lokittaminen niin tietojen katselun, tallennuksen, muuttamisen kuin poistamisenkin osalta.

Yksi erityinen sovellukseen toteutettava piirre koskee vaatimusta ilmoittaa rekisteröidylle toiselta rekisterinpitäjältä saaduista tiedoista: mikäli henkilötietoja vastaanotetaan toiselta rekisterinpitäjältä ilman, että tietojen saamiseen on lakisääteinen oikeus tai tiedot ovat luottamuksellisia, tulee rekisterinpitäjän ilmoittaa saaduista tiedoista rekisteröidylle

kuukauden sisällä joko ensimmäisen yhteydenoton yhteydessä, tai jos tällaista yhteydenottoa ei luonnollisesti synny, muilla konstein. Rekisterinpitäjän on siis huolehdittava siitä, että käyttötapaukset sisältävät myös kyseisen ilmoitusvelvollisuuden huomioinnin. Toinen erityisvaatimus on sen selvittäminen, ketkä käyttäjät ovat käsitelleet tietyn henkilön henkilötietoja. Lisäksi lokien avulla tulisi pyrkiä, kuten muissakin tapauksissa, löytämään mahdolliset poikkeavat haut ja toimenpiteet, jotka kohdistuvat henkilötietoihin.

Tässä vaiheessa on kuvattava havaitut tarpeet sekä säännöllisille, määrämuotoisille tiedonluovutuksille että tiedon vastaanotoille toisten rekisterinpitäjien järjestelmistä tarkoitukseen soveltuvien ratkaisujen löytämiseksi. Tiedonluovutukset voidaan jakaa rekisteröidylle itselleen tehtäviin luovutuksiin ja rekisteröidyn tietojen luovuttamiseen kolmansille osapuolille. Rekisteröidyn oikeuksiin kuuluu saada itsestään rekisterinpitäjän henkilörekisteriin tallennetut tiedot joko selväkielisessä tai sähköisesti luettavassa muodossa, joten nämä käyttötapaukset tulee huomioida toteutuksen määrittelyssä. Kolmansille osapuolille luovutettavien tietojen osalta taas on huomioitava henkilötietojen minimointi: rekisteröidystä saa luovuttaa vain käyttötarkoituksen kannalta relevantit tiedot. Arkaluonteisten tietojen luovuttaminen ei ole sallittua kuin erikoistapauksissa. Mikäli tiedonluovutuksen kohteena on viranomaisen julkinen asiakirja, ei luovutuksen vastaanottajaa ole välttämättä mahdollista rekisteröidä. Jos sen sijaan kyse on sopimukseen tai lakisääteiseen velvollisuuteen perustuvasta sähköisestä tiedonluovutuksesta, tulee rekisteröidyn henkilötietojen luovutuksesta aina jäädä merkintä lokitietoihin. Kyseistä tietoa tarvitaan, mikäli rekisteröity käyttää oikeuttaan tietojen poistamiseen tai tiedonkäsittelyn rajoittamiseen, jolloin rekisterinpitäjän velvollisuutena on ilmoittaa tiedonluovutuksen saajille oikeuden käyttämisestä. Tämä vaatii lisäksi joka tiedonluovutuksen yhteydessä tietojen vastaanottajan tunnistamista. Myös tiedonluovutusten osalta on pyrittävä löytämään mahdolliset poikkeavat tiedonluovutuspyynnöt tai rajapintakyselyt teknisin keinoin.

Rekisterinpitäjällä on velvollisuus huolehtia rekisteröityjen tietojen oikeellisuudesta ja ajantasaisuudesta mahdollisuuksien mukaan. Sovellusarkkitehtuurin arkkitehtuurikomponenteiksi tulee siksi tunnistaa niin toisilta rekisterinpitäjiltä saatavat henkilötiedot kuin mahdolliset muut sähköiset palvelut, joiden avulla henkilötietoja voidaan tarkistaa ja päivittää. Tällaiseksi palveluksi voidaan lukea esimerkiksi Digi- ja väestötietoviraston ylläpitämä Väestötietojärjestelmä, jonka kautta on saatavissa Suomen kansalaisten ja Suomessa kirjoilla olevien ulkomaalaisten henkilötietoja.

Henkilötietojen poistaminen säilytysajan ja -tarpeen päätyttyä on yksi tärkeimmistä rekisterinpitäjän velvollisuuksista. Vaiheessa B on päätetty, kauanko henkilötietoja on

lainsäädännön mukaan ja organisaation tarpeisiin nähden säilytettävä, ja tämä on nyt huomioitava sovellusarkkitehtuurin suunnittelun yhteydessä. Henkilötietojen poistaminen voidaan tehdä joko poistamalla tiedot fyysisesti levyltä tai anonymisoimalla ne. Anonymisointi on soveltuva tapa tietojen poistoon tilanteessa, jossa henkilötietoihin liittyvät muut tiedot tai esimerkiksi tapahtumalukumäärät halutaan edelleen säilyttää tilastointi- tai arkistointitarpeita varten. Tällaisessa tapauksessa on henkilötiedot todennäköisesti mahdollista täysin irrottaa varsinaisen säilytettävän tiedon yhteydestä. Jos tämä ei ole mahdollista, voidaan harkita pseudonymisointia: poistetaan varsinaiset suorat henkilötiedot, mutta jätetään jäljelle epäsuoria henkilötietoja pyrkien minimoimaan mahdollisuus tunnistaa rekisteröity. Toimivia menettelytapoja ovat myös tietojen ylikirjoittaminen tai merkitseminen poistetuiksi niin, että se estää niiden käyttämisen sovelluksessa siihen asti, kunnes ne fyysisesti poistetaan [30]. Sovellusarkkitehtuuriin tulee sisällyttää poistomenettelyt, jotka poistavat henkilötiedot sovitulla tavalla automaattisesti henkilötiedon säilytysajan päätyttyä. Tässä yhteydessä on huomioitava perustiedon säilytyksen lisäksi myös muut mahdolliset säilytyspaikat kuten tiedonsiirtoon käytetyt levyjaot ja välitaulut sekä henkilötiedon kopiot muissa henkilörekistereissä. Henkilötietojen poistaminen tulee aina lokittaa.

Myös lokitietojen ja varmistusten säilytysaikoihin on kiinnitettävä huomiota, jotta niihin tallennetut henkilötiedot eivät säily pitempään kuin mikä on varsinaisten henkilötietojen säilytysaika. Jos varmistusten säilytysaika on pitempi kuin henkilötietojen säilytysaika tietojärjestelmässä, on tämä huomioitava varmistusten palautusmenettelyjen suunnittelussa: varmistuksen palauttamisen jälkeen täytyy olla mahdollista poistaa datasta ne henkilötiedot, jotka on tuotannossa poistettu kyseisten varmistusten ottamisen jälkeen. [30]

Sovellusarkkitehtuurikuvauksessa tulee tämän vaiheen jälkeen olla kuvaukset liittyen sovellusarkkitehtuurin arkkitehtuurikomponentteihin, joiden avulla tehdään henkilötietojen käsittelyä kuten rekisteröidyn käyttöliittymä ja henkilötietojen käsittelijän käsittelysovellus, henkilötietojen käsittelytoimintoihin, käyttäjäroolien oikeuksiin sekä havaittuihin tiedonsiirtoihin ja -luovutuksiin. Kuvausmallit valitaan kohteena olevan arkkitehtuurimuutoksen mukaan: arkkitehtuurikuvaukseen voidaan sisällyttää esimerkiksi sovellus- ja rajapintaportfoliot, matriisit toiminnoista käyttäjärooleittain tai sovellusten välisestä vuorovaikutuksesta sekä kaavioita kuten UML-käyttötapauskaavion, moduulikaavion tai systeemikontekstikaavion. On huomattava, että tässä vaiheessa ei vielä kuvata toteutusta erityisen tarkasti, vaan vasta määritellään tarvittava arkkitehtuuri ja sen komponentit. Varsinaiset ratkaisukomponenttikohtaiset kuvaukset tehdään sovelluskehitysvai-

heessa. [24]

Yhteenveto C2. Sovellusarkkitehtuuri -vaiheen sisäänrakennettuun tietosuojaan liittyvistä tehtävistä:

- Rekisteröidyn tarvitsemien sovelluspalveluiden kuvaaminen
- Henkilötietojen käsittelijän tarvitsemien sovelluspalveluiden kuvaaminen
- Käyttäjäroolien sovellusoikeuksien kuvaaminen
- Tiedonsiirtojen ja -luovutusten arkkitehtuuriratkaisujen kuvaaminen
- Poistomenettelyjen kuvaaminen

4.2.4 Teknologia-arkkitehtuurin kehittäminen

Teknologia-arkkitehtuuriin liittyvät sisäänrakennetun tietosuojan vaatimukset koskevat teknisten ympäristöjen tietoturvaa, eivätkä ne poikkea normaaleista tietoturvavaatimuksista. Moniin teknologiaan vaikuttaviin vaatimuksiin on otettu kantaa sovellusarkkitehtuurin suunnittelun yhteydessä: tunnistautuminen, käyttövaltuudet ja lokitus ovat nousseet esiin jo vaiheessa C, mutta ne tulee ottaa huomioon myös vaiheessa D, jotta niiden vaatimat tekniset ratkaisut tulevat kuvattua.

Teknologia-arkkitehtuurin peruskomponenttien kuten palvelinten, verkkojen, integraatiopalveluita tarjoavien palveluväylien ja tietoliikenteen osalta sisäänrakennetun tietosuojan vaatimukset tulevat käytännössä täytettyä, kun organisaatio huolehtii teknisen ympäristönsä normaaleista tietoturvatarpeista hyvin. Asiattoman pääsyn estäminen ja tietoliikenneyhteyksien suojaaminen ja salaaminen sekä turvallinen verkkoarkkitehtuuri ovat tietoturvan perusvaatimuksia, kuten myös tietojenkäsittely-ympäristön vikasietoisuus ja palautumiskykyisyys. Tämä voi tarkoittaa esimerkiksi palvelun palvelinten ja tietoliikenteen kahdentamista tarvittaessa, mutta vähintäänkin varmistusten ja niiden palauttamisen suunnittelua. Tietosuoja-asetuksessa esiin nostettu riskilähtöisyys koskee varsinkin teknologiaympäristön tietoturvan ja sisäänrakennetun tietosuojan vaatimuksia: on arvioitava, mitä on riittävä tietoturvatoimenpiteiden taso kussakin ympäristössä. Internetiin avoinna olevat palvelut vaativat erilaisia tietoturvatoimenpiteitä kuin organisaation sisäiset palvelut.

Käyttövaltuuksilla ja pääsynhallinnalla on teknologia-arkkitehtuurissa suuri merkitys. Tekniseen ympäristöön pyrkivät käyttäjät ja sinne tehtävät rajapintakutsut on voitava

tunnistaa pääsynhallinnassa, jotta voidaan estää mahdolliset ulkopuolelta tulevat henkilötietojen tietoturvaloukkausyritykset. Pääsynhallinnan on huomioitava myös mahdolliset etäkäyttöyhteydet EU:n tai ETA:n ulkopuolelta, koska mikäli etäyhteyksien yli käsitellään henkilötietoja, on se laskettava tiedonluovutukseksi, mikä on kolmansien maiden osalta tietosuoja-asetuksessa hyvin rajattua [30]. Teknologiakomponenttien, esimerkiksi palvelinten ja tietokantojen, käyttöoikeudet on rajattava mahdollisimman hyvin niin, ettei ympäristöön pääse asiattomia henkilöitä eivätkä ympäristössä työskentelevät it-asiantuntijat pääse käsittelemään henkilötietoja tarpeettomasti. Käyttöoikeuksien osalta on arvioitava myös, tuleeko ympäristössä työskentelemään it-asiantuntijoita oman organisaation ulkopuolelta. Mikäli esimerkiksi sovellustoimittajan sovelluskehittäjillä on pääsy ympäristöön, joissa säilytetään ja käsitellään todellisia henkilötietoja, on tämä huomioitava käyttövaltuuksien lisäksi sopimuksissa. Oikeuksien rajaaminen voi toisinaan kuitenkin olla vaikeaa ilman, että työskentely estyy tai hankaloituu. Siksi teknisenkin ympäristön operoinnissa on syytä noudattaa lokittamisen periaatetta ja kirjata lokiin palvelimelle kirjautumiset ja siellä tehdyt toimenpiteet ja sinne kohdistuvat tietoliikennekutsut. Jos käytetty tietokantatuote tukee suorien tietokantatoimenpiteiden kuten sql-operaatioiden lokittamista, on tätä toiminnallisuutta syytä hyödyntää henkilötietoja sisältävien tietokantataulujen osalta. Lisäksi henkilötietojen tallentamista salatussa muodossa on syytä harkita.

Tietojärjestelmien kehittämiseen on tyypillisesti käytettävissä vähintään kolme eri ympäristöä: kehitysympäristö, jossa sovelluskehitystä tehdään, testiympäristö, jossa sovellukset testataan, ja tuotantoympäristö, jossa niitä käytetään. Varsinkin tilanteessa, jossa sovelluskehitystä tekee ulkopuolinen toimija, on syytä miettiä, onko kyseisillä toimijoilla tarvetta päästä tuotantoympäristöön ja sen kautta käsittelemään tuotannon henkilörekistereissä olevia henkilötietoja. Jos tämä voidaan sulkea pois, on tarkkaan harkittava, miten henkilötiedot esitetään kehitys- ja testiympäristöissä. Pyrkimyksenä tulee olla, ettei niihin kopioida todellisia henkilötietoja, vaan käytetään joko tekaistuja henkilötietoja tai, mikäli tietojärjestelmän sisältö on moniulotteinen ja toimivan testidatan tuottaminen on muuten vaikeaa, vähintäänkin mahdollisuuksien mukaan niin kutsuttua sotkettua dataa, jossa henkilötiedot on pseudonymisoitu korvaamalla suoria henkilötietoja joko keksityillä tai toisten henkilöiden tiedoilla. Teknologia-arkkitehtuuriin voidaan lukea tämän tyyppinen kyvykkyys muokata tuotantotiedoista pseudonymisoitua testidataa valmiiden algoritmien ja sovittujen käytänteiden avulla. On huomattava, että mikäli myös kehitys- ja testiympäristöissä on käytössä oikeellista henkilötietoa, tulee säännölliset henkilötietojen poistomenettelyt sekä täydelliset henkilötietojen käsittelyn lokitukset ja seurannat ulottaa

myös kyseisiin ympäristöihin.

Teknologia-arkkitehtuurissa on luonnollisesti otettava myös huomioon tarvittavat ulkoiset integraatiotarpeet eli tietoliikenne- ja tiedonsiirtoyhteydet ulkoisille toimijoille säännöllisten tiedonluovutusten, palvelurajapintojen ja toisilta rekisterinpitäjiltä saatavien henkilötietojen osalta. TOGAFin periaatteena on käyttää mahdollisuuksien mukaan olemassa olevia resursseja ja rakennuskomponentteja arkkitehtuurin kehittämisen yhteydessä. Siksi myös teknologia-arkkitehtuurin määrittelyssä on syytä ensisijaisesti hyödyntää organisaatiossa jo käytössä olevia, edelleen relevantteja teknisiä ratkaisuja, joiden rinnalle kehitetään tarvittaessa uusia, yleiskäyttöisiä teknologiapalveluita.

Teknologia-arkkitehtuurikuvauksiin sisällytetään kuvaukset tietoturvatoimenpiteistä, jotka samalla toteuttavat sisäänrakennettua tietosuojaa. Lisäksi kuvataan tarvittavat arkkitehtuurikomponentit ja käytettävät teknologiat sekä vaadittavat käyttövaltuusrajaukset. Kuvausmalleina voi käyttää luettelomuodon lisäksi muun muassa ympäristö- ja sijoittelukaavioita sekä tietoliikenne- ja kommunikaatiokaavioita. [24]

Yhteenveto D. Teknologia-arkkitehtuuri -vaiheen sisäänrakennettuun tietosuojaan liittyvistä tehtävistä:

- Teknisen ympäristön arkkitehtuurikomponenttien määrittely
- Tietoturvatoimenpiteiden määrittely riskilähtöisesti
- Teknisen ympäristön käyttövaltuuksien kuvaaminen
- Kehitys- ja testiympäristöjen henkilötietojen käsittelyn kuvaaminen
- Integraatiopalveluiden kuvaaminen

5 Case: Maanmittauslaitoksen sovelluskehityksen tietosuojaohjeistus

Maanmittauslaitos on valtion virasto, jonka palveluista parhaiten tunnetaan kiinteistönomistajille tehtävät maanmittaustoimitukset kuten lohkomiset ja tilusjärjestelyt sekä karttamateriaalit. Maanmittauslaitoksen palvelut voidaan jakaa kolmeen palvelukoriin:

- Huoneistot ja kiinteistöt -palvelukorissa on maanmittaustoimitusten lisäksi kiinteistöjen ja osakehuoneistojen omistuksen ja vuokraoikeuden rekisteröintiin liittyvät tehtävät, jotka muun muassa mahdollistavat niiden käyttämisen lainan vakuutena. Maanmittauslaitokselta on myös mahdollista ostaa otteita ja todistuksia kiinteistöihin, osakehuoneistoihin ja vuokraoikeuksiin liittyen sekä selata tilastotietoja kiinteistökaupoista Suomessa. Maanmittauslaitos tarjoaa lisäksi luvanvaraista tietopalvelua kiinteistötiedoista.
- Kartat ja paikkatieto -palvelukorissa on Maanmittauslaitoksen tehtävät liittyen maastotietojen ja kartta-aineistojen tuottamiseen. Maanmittauslaitoksella on verkossa tarjolla useita karttapalveluita sekä mahdollisuus ostaa karttoja. Karttaaineisto ei sisällä henkilötietoja, joten sitä on ollut mahdollista avata avoimena datana kaikkien kiinnostuneiden käyttöön.
- Tutkimus-palvelukorissa sijaitsee Maanmittauslaitoksen tutkimusyksikkö Paikkatietokeskus (Finnish Geospatial Research Institute FGI), joka tekee paikkatietoalan tutkimusta ja tutkimustiedon soveltamista käytäntöön. Paikkatietokeskus tarjoaa erilaisia asiantuntijapalveluita muun muassa koordinaattilaskentaan, kalibrointiin, paikantamiseen ja kaukokartoitukseen. [23]

Henkilöstöä Maanmittauslaitoksessa on hieman alle 1700. Työntekijöistä noin 75 % työskentelee Maanmittauslaitoksen ydintehtävissä sen tuotantoyksiköissä. Maanmittauslaitoksen tehtävistä on säädetty erillislainsäädännöllä. Suomalaisista perusrekistereistä kiinteistörekisteri, lainhuuto- ja kiinnitysrekisteri, osakehuoneistorekisteri ja kiinteistöjen kauppahintarekisteri sekä yksityistierekisteri ovat Maanmittauslaitoksen vastuulla.

It-palveluita tuotetaan Maanmittauslaitoksen it-palvelukeskuksessa (MITPA). Varsinaista sovelluskehitystä tehdään MITPAn Sovelluspalvelut-tulosyksikössä, jossa työskentelee noin 80 henkilöä. Lisäksi Paikkatietokeskuksella on omaa sovellustuotantoa. Maanmittauslaitos toteuttaa itse pääosan tietojärjestelmistään, mutta käyttää toteutustyöhön enenevässä määrin myös ulkoisia sovellustoimittajia. Viraston käytössä on myös jonkin verran valmisohjelmistoja. Maanmittauslaitoksen tietojärjestelmäluettelossa on noin 180 tietojärjestelmää, sovellusta tai it-palvelua, joista noin 2/3:aan liittyy henkilötietojen käsittelyä. Merkittävä osuus Maanmittauslaitoksen antamasta tietopalvelusta tuotetaan 23 rajapintapalvelun kautta laissa kiinteistötietojärjestelmästä ja siitä tuotettavasta tietopalvelusta (453/2002) nimetyille viranomaisille sekä hakemuksen perusteella luvan saaneille organisaatioille, joiden toimiala liittyy kiinteistöihin [18]. Osa rajapintapalveluista on avoimia, mutta näihin ei koskaan liity henkilötietojen luovutusta. Myös osakehuoneistoihin liittyen on tulossa käyttöön rajapintapalveluita. [22]

5.1 Tietosuojatyö Maanmittauslaitoksessa

Maanmittauslaitos toteutti vuosina 2016–2018 kaksi projektia liittyen tietosuoja-asetukseen ja sen täytäntöönpanoon [22]. Ensimmäinen tietosuojaprojekti oli esiselvitysprojekti, jossa selvitettiin Maanmittauslaitosta koskevasta lainsäädännöstä säädökset, joilla on vaikutusta henkilötietojen käsittelyyn, ja suunniteltiin varsinaista toimeenpanoprojektia. Esiselvityksen yhteydessä todettiin, että Maanmittauslaitoksessa tehtävä henkilötietojen käsittely perustuu pääsääntöisesti rekisterinpitäjän lakisääteisen velvoitteen noudattamiseen. Erityislainsäädännön osalta todettiin, että varsinkin tutkielman alussa käsitelty laki viranomaisen asiakirjojen julkisuudesta eli julkisuuslaki vaikuttaa Maanmittauslaitoksen henkilötietojen käsittelyyn luovutettavien asiakirjojen sisältämien henkilötietojen osalta.

Myöhemmässä projektissa valmistauduttiin tietosuoja-asetuksen velvoittavaksi tulemiseen muun muassa sopimuskäytäntöjen ja hankintaohjeistuksen uusimisen, henkilöstön ohjeistuksen ja koulutuksen sekä tietosuojaselosteiden tarkistamisen avulla. Myös lokienhallinnan ja riskienhallinnan politiikat tarkistettiin ja ohjeistusta lisättiin. Projektin aikana toteutettiin lisäksi henkilötietoinventaario kaikista Maanmittauslaitoksen sähköisistä tietovarannoista ja niitä käsittelevistä sovelluksista, ja tietojen analysoinnin jälkeen kullekin tietojärjestelmälle tehtiin toimenpidesuunnitelma sen saattamiseksi tietosuoja-asetuksen mukaiseksi. Projektin aikatauluhaasteiden vuoksi ei projektissa kuitenkaan eh-

ditty toteuttaa ohjeistusta tulevien sovelluskehitysprojektien tueksi. Tietoturvallisuuteen, käyttövaltuushallintaan ja lokitukseen liittyviä ohjeita on Maanmittauslaitoksessa dokumentoitu muun muassa teknologiakäsikirjaksi kutsuttuun dokumentaatioon, missä myös viitataan sisäänrakennetun tietosuojan vaatimukseen, mutta ohjeistoa, jossa olisi huomioitu tietosuoja-asetuksesta sovelluskehitykselle tulevat sisäänrakennetun tietosuojan vaatimukset, ei ole vielä olemassa. Tätä puutetta on omalta osaltaan pyritty paikkaamaan tällä tutkielmalla. [22]

Henkilötiedon käsite sekä suoran ja epäsuoran henkilötiedon määrittäminen lienee organisaatioille normaalisti melko helppoa. Maanmittauslaitoksessa on jouduttu kuitenkin julkisuuslain asettamien velvollisuuksien vuoksi pohtimaan, milloin henkilötieto onkin julkista tietoa, johon ei sovelleta tietosuoja-asetusta. Käytännössä pohdinta on koskenut kiinteistötunnusta. Kiinteistötunnus on kunkin Suomessa olevan kiinteistön yksilöivä tunniste, jonka perusteella voi muun muassa hankkia Maanmittauslaitokselta julkisia asiakirjoja, joista ilmenee myös kiinteistön omistajan tiedot. Kiinteistötunnuksilla on myös osoite, joka tyypillisesti luetaan henkilötiedoksi. Kiinteistötunnus on nykyään rajoituksitta saatavilla esimerkiksi Maanmittauslaitoksen verkkosivuilla olevasta sähköisestä karttapalvelusta. Hallituksen esityksessä HE 102/2015 on todettu, ettei kiinteistötunnuksen luovutus avoimesti ilman lupaa heikennä henkilötietojen suojaa. Tämän vuoksi on Maanmittauslaitoksessa perustellusti tulkittu, ettei kiinteistötunnusta tai muuta vastaavaa kohdetunnusta voida yksinään pitää sellaisena henkilötietona, johon sovellettaisiin tietosuoja-asetuksen mukaisia henkilötietojen käsittelyä koskevia vaatimuksia ja rekisteröidyn oikeuksia. Tämän määrittelyn vuoksi on Maanmittauslaitoksessa todettu, ettei kiinteistötunnuksen tai sen perusteella hankittavan asiakirjan luovuttaminen ole henkilötiedon luovuttamista eikä näin ollen sitä myöskään tarvitse lokittaa. [22]

Toinen Maanmittauslaitokselle hankala henkilötiedon määritelmä on paikkatiedon määrittely henkilötiedoksi. Ympäristöministeriö on julkaissut raportin 10/2018, jossa aiheena on tietosuojalainsäädännön vaikutukset paikkatiedon julkaisemiseen. Raportissa on todettu, ettei karttoja käsitellä henkilötietoina, vaikka niistä ilmenisi osoite tai kiinteistön rekisterinumero, jonka avulla yksittäisen henkilön asuttama rakennus tai omistama kiinteistö voidaan selvittää. Tiedon hyödyllisyys ja tarpeellisuus sekä pitkäaikainen yleinen käyttö verrattuna epäsuoraan henkilötietoon, jona karttatietoakin voidaan pitää, on tässä tapauksessa etusijalla [15]. Maanmittauslaitoksella on lakisääteisen tehtävänsä vuoksi runsaasti paikkatietoa rekistereissään. On kuitenkin tulkittu, että koska kyseessä ei koskaan ole henkilöiltä kerätty sijaintitieto, vaan paikkatietoa käytetään aina nimenomaan kart-

tatietona, ei Maanmittauslaitoksessa ole tässä vaiheessa paikkatietoja, joita luettaisiin tietosuoja-asetuksen piiriin. Tämä ei kuitenkaan tarkoita sitä, etteikö uusien paikkatietorekisterien kohdalla jouduttaisi aina harkitsemaan tiedon luonnetta.

Maanmittauslaitoksen tietosuojatyö on tällä hetkellä hyvin linjassa sen kanssa, mihin projektit päätyivät vuonna 2018. Projektien aikana tehdyt uudistukset esimerkiksi sopimusja hankintaprosesseihin ovat edelleen voimassa. Maanmittauslaitoksessa on tietosuojavastaava ja tietosuojaryhmä, jotka koordinoivat tietosuojatyötä koko viraston tasolla. Sovelluskehityksen tietosuojatyötä ei kuitenkaan ole vastuutettu, minkä vuoksi sen ohjeistaminen ja määrämuotoistaminen ei ole edennyt. Koska projekteissakaan ei aikataulusyistä ehditty tarkemmin perehtyä sovelluskehityksen vaatimaan tietosuojaohjeistukseen, on nyt tehty työ sisäänrakennetun tietosuojan vaatimusten keräämiseksi jatkumoa projekteissa kesken jääneelle työlle sisällyttää tietosuoja automaattiseksi osaksi Maanmittauslaitoksen sovelluskehitystyötä. [22]

5.2 Haastattelutulokset

Tutkielman toisena päätavoitteena oli selvittää, minkälaista ohjeistusta sovelluskehittäjät tarvitsevat sisäänrakennetun tietosuojan vaatimusten huomioimiseksi sovelluskehityksessä.

Tämän tavoitteen selvittämiseksi haastateltiin 19 Maanmittauslaitoksen sovelluskehityksen asiantuntijaa. 11 haastatelluista oli Sovelluspalveluiden ja Paikkatietokeskuksen palvelupäälliköitä ja muita asiantuntijoita, joiden vastuulla olevissa tietojärjestelmissä käsitellään henkilötietoja. Lisäksi haastateltiin kahdeksaa teknologiaympäristön, lokituksen tai kokonaisarkkitehtuurin asiantuntijaa. Haastatteluissa kysyttiin seuraavia asioita:

- Mihin tietosuojaan liittyviin vaatimuksiin tarvitaan/ei tarvita ohjeita/periaatteita?
- Minkä tasoista ohjeistusta tarvitaan?
- Mikä olisi sopiva paikka ohjeistukselle?
- Mitä tietosuojakeinoja tunnistat jo käytetyn MML:ssa/MML:n palveluissa?
- Mitä keinoja lisäisit listalle?
- Millä teknisillä toimenpiteillä olisi mahdollista tukea henkilötietojen tietoturvaloukkausten havaitsemista?

- Miten sovelluskehityksessä huomioidut tietosuojavaatimukset tulisi dokumentoida?
- Missä päätökset sovelluskehityksen tietosuojatoimenpiteistä tulisi tehdä?
- Mitä muuta mieleesi tulee tietosuojaan ja henkilötietojen käsittelyyn liittyen?

Haastatteluissa todettiin, että tietosuojan huomioiminen sovelluskehityksessä on tällä hetkellä ainakin osittain reaktiivista. Asiantuntijat selvittävät toisiltaan, miten tietosuojavaatimukset on eri palveluissa ratkaistu. Halua tehdä asiat samalla tavalla on, mutta ei yhteenkoottua tietoa siitä, miten organisaatiossa tietosuojaominaisuudet implementoidaan järjestelmiin. Olemassa oleva ohjeistus on hajallaan eri sijainneissa: intranetissä, asianhallintajärjestelmässä rajatuin käyttöoikeuksin ja organisaatiowikissä joskus usean eri otsikoiden alla. Samasta aiheesta on kirjoitettu ohjeistusta useampaankin paikkaan, jolloin tuorein tieto saattaa jäädä havaitsematta. Arkkitehtuurikomponenteista, joiden käyttö on jo ohjeistettu, tulee niiden asiantuntijoille kyselyitä, mikä kertoo siitä, ettei olemassa olevia ohjeita joko löydetä tai niitä ei lueta. Lisäohjeistusta ja ohjeiden keskittämistä pidettiin ehdottoman tarpeellisena, jotta sisäänrakennetun tietosuojan vaatimus tulisi täytettyä organisaation haluamalla tavalla.

Eräs haastateltu totesi, että ohjeita tarvitaan pääasiassa siinä vaiheessa, kun kehittämistyötä suunnitellaan, koska silloin tulee tehdä tärkeimmät päätökset henkilötietojen käsittelyyn liittyen. Silloin on mahdollista taklata ongelmia, jotka muuten saattavat tulla vastaan vasta sovelluskehitysvaiheessa. Tällöin on tarpeen tunnistaa strategiasta ja ohjaavasta lainsäädännöstä tarvittavat kriteerit ja reunaehdot tietosuojakäsittelyllä. Myös sen arviointiin, mikä on henkilötietoa, tarvitaan toisinaan apua esimerkiksi paikkatiedon osalta. Tietosuojaohjeistuksesta on hyvä löytyä valmiit tietosuojavaatimukset, jotka tulee huomioida käyttötapauksissa ja muussa määrittelyssä. Tarve tällaiselle vaatimuspankille nousi esiin useammassakin haastattelussa. Todettiin, että vaatimukset on kuitenkin valittava vaatimuspankista sen mukaan, mitkä prosessit ja toimijat ovat sidosryhminä kehittämisen kohteena olevassa tietojärjestelmässä, mitä tietovirtoja ja henkilötietoryhmiä siinä käsitellään, sekä mikä on tietojärjestelmän suojaustasovaatimus ja luonne. Yksi ehdotus oli esittää kehittäjille tarkoitettu ohjeistus agile-menetelmistä tuttuna valmiin määritelmänä (Definition of Done, DoD) lisättynä toteutusohjeistuksella, määrittelijöille ja testaajille taas vaatimukset voi esittää testitapauksina. Käytännössä suunnitteluprosessi etenee vaiheittain eri sidosryhmien kanssa työtä tehden, jolloin myös ohjeistus voi erikseen huomioida substanssiasiantuntijoiden kanssa tehtävät päätökset, kokonaisarkkitehtien kanssa vedettävät suuntaviivat ja kehittäjien kanssa sovittavat toteu-

tusvaatimukset. Kuten eräs haastateltu sanoi: ”Ei heti kaikkea, vaan järjestyksessä, mitä pitää tehdä.” Tämä ’eri ohjeet eri sidosryhmille’-ajatus esiintyikin useammassa haastattelussa. Maanmittauslaitoksen oman ohjeistuksen lisäksi toivottiin sen yhteyteen linkkejä keskeisiin tietosuojaan liittyviin suosituksiin ja valtionhallinnon ohjeisiin.

Ohjeilla tulee olla yksi keskitetty sijoituspaikka, johon tarvittaessa viitataan muista ohjeista. Eräs haastatelluista totesi näin: ”Oleellista olisi, että tietosuoja-asiat tulisivat väkisin vastaan jossain prosessissa.” Tärkeää on siis löytää myös ne toimintaohjeet, joista tulee päästä tietosuojaohjeistoon. Näitä toimintaohjeita ovat muun muassa projekti- ja teknologiakäsikirjat [22]. Eräs haastateltava toivoi ohjeistolle wikimäistä, verkostomaista dokumentointimallia, josta tarvittavat ohjeet on helposti löydettävissä hauilla.

Prosessien, sidosryhmien ja tietovarantojen välisten tietovirtojen dokumentointiin toivottiin mallia. Tietomallien kuvaamisen pitäisi olla standardikielellä kuten UML:llä toteutettua. Tietovirtojen avulla nähdään myös tietojärjestelmäprosessi eli miten tieto virtaa tietojärjestelmästä ja -varannosta toiseen. Kuvauksista tarvitaan niin looginen kuin fyysinen taso. Tärkeää on kuvata, missä eri henkilötietojen perustieto sijaitsee ja minne kaikkialle se kopioituu, jotta voidaan muun muassa arvioida sen poistamiseksi vaadittavat toimenpiteet. Uuden palvelun kuvaaminen sekä nyky- että tavoitetilan osalta heti suunnittelun alussa antaa käsityksen siitä, minkälaisesta kehittämistyöstä on kyse. Kokonaisarkkitehtuuriasiantuntijoiden on hyvä olla mukana kehitysprojekteissa koko arkkitehtuurisuunnittelun ajan.

Riskienarvioinnista todettiin myös tarvittavan ohjeistusta. On mahdollista, että riskienarvioinnista puhuttaessa se sekoitetaan projektiriskien hallintaan, joka koskee kuitenkin vain projektinaikaisia riskejä. Tietojärjestelmän riskienarvioinnilla tavoitellaan tulevien tuotannonaikaisten riskien löytämistä. Pari haastateltavaa toivoi ohjeita riskienarvioinnin havainnoista ja tietoturvatestauksen poikkeamista juontuvien toimenpiteiden dokumentointiin ja toteutuksen seurantaan. Yksi haastatelluista toivoi myös kuvausta siitä, mikä on vanhoihin tietojärjestelmiin jälkikäteen tehtävien tietosuojaominaisuuksien minimitaso.

Varsinaisesti sovelluksen teknologiaan liittyvän ohjeistuksen ei katsottu olevan välttämättä tarpeen. Teknologiariippumaton ohjeistus on mahdollista viedä riittävän tarkalle tasolle. Teknologiaan ripustettujen ohjeiden toteutus pitävästi sen sijaan on vaikeaa, koska teknologioita on monia. Yhden haastatellun sanojen mukaan ”liiketoimintatasoisen ohjeistuksen tulisi riittää”.

Yksi esille nousseista asioista oli käyttäjäroolien määrittely: mitä ja miten eri

käyttäjäroolit saavat henkilötietoja käsitellä. Ohjeita tarvitaan muun muassa arkaluonteisten henkilötietojen käsittelyn toteuttamiseen tietojärjestelmään niin tietokannan, käyttöliittymän kuin tulosteiden osalta. Tietosuoja-asetuksessa ei ole erikseen mainittu turvakieltoa tai yhteystietojen salassapitopäätöstä, mutta niiden huomiointi henkilötietojen käsittelyn yhteydessä on valtion virastossa tärkeää. Turvakiellolla tarkoitetaan Digi- ja väestötietovirastolta haettavaa turvaamistoimea, jolla voidaan rajoittaa henkilötietojen luovuttamista väestötietojärjestelmästä tilanteessa, jossa on perusteltua olettaa henkilön tai hänen perheensä terveyden tai turvallisuuden olevan uhattuna [4]. Maanmittauslaitos saa väestötietojärjestelmästä tiedon rekisteröidyn turvakiellosta ja sen voimassaolon päättymispäivämäärästä käytössään olevien integraatioiden avulla. Yhteystietojen salassapitopäätös puolestaan on päätös, jonka rekisteröity voi hakea erikseen yksittäiseltä julkishallinnon toimijalta. Tämä perustuu julkisuuslaissa olevaan lainkohtaan, jonka mukaan henkilön on mahdollista pyytää yhteystietojensa salaamista julkisista asiakirjoista, mikäli hänellä on perusteltu syy olettaa terveytensä tai turvallisuutensa olevan uhattuna [19](24 §). Päätös on käytännössä pysyvä. Näiden osalta tarvitaan ohjeistusta siitä, mitä tietoja kyseisistä rekisteröidyistä on oikeus tallentaa ja missä tietoja on oikeus hyödyntää. Haastattelussa esitettiin myös toivomus sen kuvaamisesta, miten ulkopuoliset sovelluskehittäjät, jotka osallistuvat kehitystiimin työhön, saavat käsitellä henkilötietoja esimerkiksi häiriötilanteiden selvittämiseksi.

Kehittäjille tarkoitetun ohjeistuksen tulee olla helposti omaksuttavissa, helposti saatavilla ja tarjottavissa käyttöön myös ulkoisille sovellustoimittajille. Sen osalta tarvitaan sovellussuunnitteluohjeita, koodausohjeita, käyttöoikeuksien hallintaan, pääsynhallintaan ja lokitukseen liittyviä ohjeita. Tarkastus- tai muistilista-tyyppistä ohjeistusta pidettiin useammassa haastattelussa hyvänä ratkaisuna, koska se on tiivis ja ytimekäs tapa esittää asiat. Toisaalta toivottiin myös FAQ-tyylistä usein kysyttyjen kysymysten ohjemallia esimerkiksi tiettyyn rakennuskomponenttiin kuten tietokantaan liittyen. Sovelluskehittäjien ohjeiden luokittelussa eri aiheisiin voi ottaa mallia teknologiakäsikirjan rakenteesta. Erikseen nostettiin esiin lokittaminen ja sen ohjeistaminen, mitä henkilötietojen käsittelystä tulee lokittaa. Teknologia-asiantuntijat toivoivat, että ohjeissa muistutettaisiin ottamaan teknologia-asiantuntijat mukaan suunnitteluun jo teknologia-arkkitehtuurin suunnitteluvaiheessa.

Käyttöliittymäsuunnittelun osalta ehdotettiin tietojen ryhmittelyä eri näytöille tai välilehdille sen mukaan, mitä tietoja missäkin käyttötilanteessa ja milläkin käyttöoikeuksin on tarvetta käsitellä. Esimerkiksi näytölle, jota saatetaan näyttää myös

asiakkaalle, ei pidä tuoda tietoja, joita tämä ei saa nähdä. Henkilötiedon tyypin esittämistä metatiedoilla kuten värillä ehdotettiin: näin voitaisiin esimerkiksi arkaluonteiset henkilötiedot merkitä näytölle niiden suojelemiseksi. Myös lokittamisvaatimus voi vaikuttaa tietojen ryhmittelyyn.

Tietokantasuunnittelun osalta todettiin tietojen poistamisen vaikutukset tietokantaratkaisuun ja mietittiin, olisiko poistoa varten toteutettavissa yleistä poistoalgoritmia, jonka avulla poistot voitaisiin tehdä keskitetysti. Tietokantataulujen tietojen ryhmittelyssä on huomioitava tietojen säilytysajat. Tietojen pseudonymisoinnista ja anonymisoinnista ei ole olemassa ohjetta, mutta sellainen olisi hyvä olla esimerkiksi tilanteeseen, jossa henkilötiedot tulee jo poistaa, mutta tieto tapahtumasta tulee edelleen säilyttää tilastointia varten. Samoin testausta varten tarvittavan sotketun, pseudonymisoidun datan tuottamisesta tarvitaan ohje. Testidatassa on muistettava huomioida myös testitapaukset erityisryhmien henkilötiedoille.

Varsinaisten ohjeiden lisäksi toivottiin hyviä case-esimerkkejä siitä, miten sisäänrakennettu tietosuoja pitäisi toteuttaa tietojärjestelmiin. Tarvittavien liitännäisten rakennuskomponenttien kuten lokienhallinnan ja pääsynhallinnan implementoimiseen toivottiin helppoja kuvauksia ja käyttöönotto-ohjeita sekä vaatimuslistoja tietosuojavaatimusten tyyliin. Maanmittauslaitoksen omien yhteiskäyttöisten rakennuskomponenttien lisäksi palveluissa on syytä käyttää valtionhallinnon yleisiä tietoturvaan liittyviä palveluita kuten suomi.fi-tunnistautumista silloin, kun niitä on haluttuun tarkoitukseen olemassa. Lisäksi toivottiin tietoa siitä, mistä voi kysyä neuvoja kunkin vaatimuksen kohdalla.

Haastatteluissa listattiin Maanmittauslaitoksessa jo käytettyjä keinoja tietosuojan turvalliseksi toteuttamiseksi. Näitä keinoja ovat palvelin- ja tietoliikennevalvonnat, palomuurisäännöstöt, henkilötietojen käsittelyn ja tietojärjestelmien käytön lokitukset, erilliset debug-lokit, joiden avulla vältetään sovellustoimittajien pääsy tuotantodataan, testidatan henkilötietojen sotkeminen, käyttövaltuuksien hallinta niin sisäisille kuin ulkoisille käyttäjille, vahva tunnistaminen, henkilötietojen luovutus käyttöoikeuksien mukaan, salatun protokollan käyttö tietoliikenteessä sekä tiedon anonymisointi ja aggregointi aikasarjoihin. Keinot eivät kuitenkaan ole käytössä kaikissa palveluissa, vaan toteutus on riippunut palvelun toteutusajankohdasta ja toteuttajista. Muutamissa ei-lakisääteisissä palveluissa on myös käytössä rekisteröityminen omalla suostumuksella. Todettiin, että myös turvallisuusselvityksen teettäminen henkilöstä ja sovellustoimittajista on yksi Maanmittauslaitoksessa käytössä oleva tietoturvatoimenpide.

Henkilötietojen tietoturvaloukkausten havaitsemiseksi mietittiin tapoja. Henkilötietojen

käsittelyn lokitus on ensimmäinen keino, jonka avulla voidaan yrittää löytää vääränlaista käyttäytymistä. Normaalin sovelluskäytön lokituksen lisäksi tulee lokittaa palvelinkomennot ja tietokantoihin tehtävät suorat kyselyt, jos se on mahdollista. Lokien avulla on mahdollista pyrkiä havaitsemaan tiettyyn henkilötunnukseen kohdistuvia tai tietyllä aikavälillä normaalia enemmän tapahtuvia hakuja. Samoin on mahdollista tutkia kirjautumisyrityksiä epänormaalien kirjautumismäärien tai niiden epäonnistumisten havaitsemiseksi. Todettiin kuitenkin, että datan epänormaalit siirrot voivat olla vaikeita havaita lokien perusteella. Lokitukselleki voi kohdistua erityisiä säilytysaikavaatimuksia: toisinaan joudutaan selvittelemään hyvinkin pitkän ajan takaa, kuka tietoja on käsitellyt ja miten. Riskienarviointi, sovelluksen uhkamallinnus ja tietoturvatestaaminen tulee tehdä vähintään projektitasoisissa kehityshankkeissa. Maanmittauslaitoksella on käytössä valvontoja ja muita teknologiakomponentteja, joiden avulla pyritään estämään ulkoisia hyökkäyksiä. Tiedonsiirrot vääriin osoitteisiin voi olla mahdollista havaita näiden avulla. Huomion kiinnittäminen vaarallisiin työyhdistelmiin olisi suotavaa.

Haastatellut miettivät myös sitä, miten valvotaan, että sisäänrakennettua tietosuojaa toteutetaan ja tehty ohjeistus ymmärretään. Yksi vaihtoehto on tehdä vaatimuksista valmiit testitapaukset, jotka käydään läpi sovelluskehityksen järjestelmä- ja hyväksymistestausvaiheissa. Lisäksi tarvitaan tietosuojaan liittyvä katselmointikäytäntö, jolla ennen sovelluskehitysvaihetta tarkistetaan, että suunnitelmissa on otettu huomioon Maanmittauslaitoksen kokonaisarkkitehtuurin mukaiset käytännöt niin tietosuojan osalta kuin muutenkin. Tiedonluovutusten osalta Maanmittauslaitoksella on oikeus auditoida sopimuskumppaneita, että nämä käsittelevät Maanmittauslaitoksen luovuttamia henkilötietoja kuten on sovittu.

Ulkopuolelta haastattelun tavoitteen esitettiin Maanmittauslaitoksen it-palvelukeskuksen johdolle toivomus sovellusarkkitehtuurikerroksen henkilöresurssien vahvistamisesta. Tällä hetkellä resurssit eivät riitä siihen, että kyettäisiin määrittämään Maanmittauslaitoksen sovelluskehitysarkkitehtuurin tavoitetila ja ohjaamaan uudet kehittämishankkeet käyttämään annettuja arkkitehtuurimäärittelyjä. Toteutusteknologioiden valintaan tarvitaan kuitenkin ennakoivaa ohjausta, jonka avulla teknologiakirjoa saadaan yhtenäistettyä ja käytetyt teknologiat dokumentoitua keskitetysti. Myös tietojärjestelmädokumentaatio vaatii parempaa yhteismitallisuutta ja vertailtavuutta. Tähän voitaisiin vastata mallipohjilla ja dokumentaatiokatselmoinneilla.

Yhteenvetona voidaan todeta haastattelusta nousseen esiin seuraavia toiveita ohjeiston toteuttamiseen liittyen:

T1 Ohjeistuksen keskittäminen yhteen sijaintiin
T2 Ohjeistuksen vaiheistaminen
T3 Ohjeiden toteuttaminen tarkistus-/muistilista- tai FAQ-muotoon
T4 Erityislainsäädännöstä tulevien kriteerien ja reunaehtojen dokumentointi
T5 Kokonaisarkkitehtuurikuvausten toteuttaminen
T6 Riskienarvioinnin ohjeistus ml. toimenpiteiden dokumentointi ja seuranta
T7 Tietosuojan toteuttamisen valvonnan käytäntöjen kuvaaminen (testitapaukset, katselmoinnit)
T8 Linkit keskeisiin suosituksiin ja valtionhallinnon ohjeisiin
T9 Valmiit vaatimukset projektien käyttöön (ns. vaatimuspankki)
T10 Ohjeiden jakaminen rooleittain: substanssi–arkkitehdit–sovelluskehittäjät
T11 Testitapausluettelo määrittelijöiden ja testaajien käyttöön
T12 Ohje ulkopuolisten sovelluskehittäjien oikeuksista käsitellä henkilötietoja

Varsinaiseen sovelluskehittäjän toteutusohjeistukseen toivottiin lisäksi seuraavia asioita:

T13 Ohje yhteisistä käytännöistä esimerkiksi rekisteröidyn oikeuksien toteuttamisessa tietojärjestelmään
T14 Ohje käyttäjäroolien määrittelystä
T15 Ohje arkaluonteisten tietojen käsittelystä ml. turvakielto ja yhteystietojen salassapitopäätös
T16 Sovellussuunnittelu- ja ohjelmointiohjeistusta kuten ohjeet henkilötietojen sijoittelusta käyttöliittymään ja tietokantasuunnittelusta
T17 Ohjeita yhteiskäyttöisten komponenttien liittämisestä sovellusarkkitehtuuriin ml. valtionhallinnon yhteiset palvelut
T18 Ohje paikkatiedon käsittelystä henkilötietona
T19 Ohje ja vaatimuslista käyttövaltuushallinnan käyttöönottamisesta
T20 Ohje ja vaatimuslista pääsynhallinnan käyttöönottamisesta
T21 Ohje ja vaatimuslista lokitusjärjestelmän käyttöönottamisesta, tarvittavista henkilötietojen käsittelyn lokituksista ja lokihälytyksistä
T22 Ohje tietoturvatoimenpiteiden käytöstä sovelluskehityksessä
T23 Ohje tietovirtojen ja henkilötietojen käsittelytoimintojen dokumentoinnista
T24 Ohje testidatan tuottamisesta, tietojen pseudonymisoinnista ja anonymisoinnista

T25 Ohje vanhoihin järjestelmiin toteutettavan tietosuojan minimivaatimuksista
T26 Case-esimerkit hyvästä tietosuojatoteutuksesta

Haastatteluista saatujen toiveiden ja ideoiden perusteella on tutkielman lopputuotoksena toteutettu Maanmittauslaitoksen sovelluskehittäjiä varten ensimmäinen versio ohjeistuksesta sisäänrakennetun tietosuojan vaatimusten huomioimiseksi sovelluskehityksessä.

5.3 Maanmittauslaitoksen tietosuojaohjeistus

Kun analysoidaan haastattelussa esille nousseita toiveita tietosuojaohjeistuksesta Maanmittauslaitoksen sovelluskehitykselle, voidaan todeta, että vain muutamat toiveista kohdistuvat siihen, miten ohjeet tulee toteuttaa, jotta ne ovat helposti hyödynnettävissä sisäänrakennettua tietosuojaa suunniteltaessa. Pääosa toiveista kohdistuu ohjeiden sisältöön: tarvitaan toteutusohjeita sovelluskehittäjille niin dokumentoinnista kuin varsinaisesta henkilötietojen käsittelytoimintojen toteuttamisesta sovelluksiin. Sovelluskehitysohjeiden tekeminen vaatii Maanmittauslaitoksen sovelluskehitysasiantuntijoiden yhteistyötä ja niin sanottujen parhaiden käytäntöjen löytämistä. Monessa tapauksessa ohjeistuksen tuottaminen vaatii myös päätöksiä siitä, mikä on organisaation tapa tehdä asiat. Näiden sisällöllisten sovelluskehitysohjeiden toteuttaminen ei kuulunut tutkielman tavoitteisiin, joten toiveet niistä jäävät odottamaan jatkokehitystä Maanmittauslaitoksessa. Muutamat toiveet eivät puolestaan ole varsinaisesti tietosuojaan liittyviä, vaan paremminkin toivomuksia tietosuojaohjeistuksen lisäksi toteutettavista ohjeista ja käytänteistä. Näiden osalta toiveet viestitään eteenpäin asiantuntijoille, jotka vastaavat niihin liittyvistä aihealueista.

Haastatteluyhteenvedossa tunnistetuista 26 ohjeistustarpeesta ja -toiveesta valittiin seitsemän toteutettavaksi ensimmäiseen sovelluskehityksen tietosuojaohjeistusrungon versioon. Kyseisiin toiveisiin viitataan tässä kappaleessa niiden tunnuksella. Toteutettavat toiveet olivat:

T1 Ohjeistuksen keskittäminen yhteen sijaintiin
T2 Ohjeistuksen vaiheistaminen
T3 Ohjeiden toteuttaminen tarkistus-/muistilista- tai FAQ-muotoon
T6 Riskienarvioinnin ohjeistus ml. toimenpiteiden dokumentointi ja seuranta

T8 Linkit keskeisiin suosituksiin ja valtionhallinnon ohjeisiin
T9 Valmiit vaatimukset projektien käyttöön (ns. vaatimuspankki)
T10 Ohjeiden jakaminen rooleittain: substanssi–arkkitehdit–sovelluskehittäjät

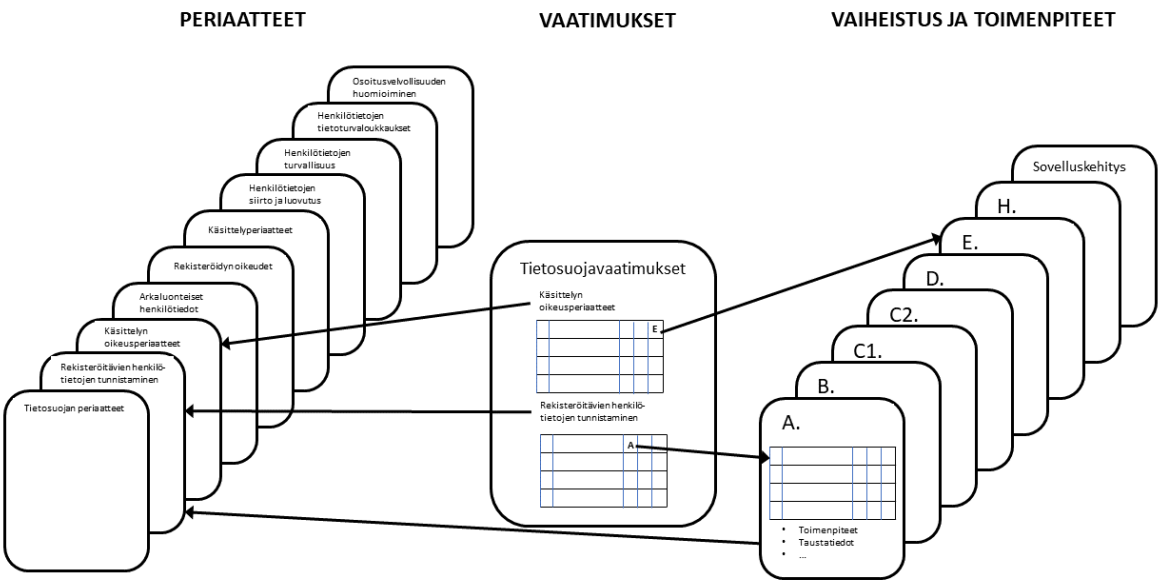
Ohjeistusrungon välineeksi valikoitui organisaatiossa jo vakiintuneessa käytössä oleva Atlassianin Confluence-organisaatiowikisovellus, koska se toimii myös organisaation tietojärjestelmädokumentaation ja muun sovelluskehitykseen liittyvän ohjeiston kuten muun muassa jo mainitun teknologiakäsikirjan sijoituspaikkana. Confluenceen perustettiin tätä ohjeistoa varten Tietosuoja sovelluskehityksessä -niminen sivualue (space), jolle kaikki ohjeistus sisäänrakennetun tietosuojan toteuttamisesta tietojärjestelmiin kerätään (toive T1).

Maanmittauslaitoksen ohjeistoon luotiin kolmenlaisia sivuja:

- Tietosuojaperiaatteet-sivut
- Tietosuojavaatimukset-sivu
- Vaihekohtaiset vaatimussivut

Näiden haastattelutulosten perusteella toteutettujen sivutyyppien väliset suhteet on kuvattu kuvassa 5.1. Kuvasta nähdään, miten eri sivutyypit ovat yhteydessä toisiinsa hyperlinkeillä.

Tietosuojaperiaatteet-sivuille on kirjoitettu kuvauksia tietosuoja-asetuksen sisällöstä. Kuvaukset on pyritty tekemään selväkielisiksi ja helposti omaksuttaviksi. Sivujen otsikot vastaavat kappaleessa 3 olevaa rekisterinpitäjän sisäänrakennettuun tietosuojaan vaikuttavien velvoitteiden jaottelua. Sivuille on kirjattu määritelmiä, luetteloita huomioitavista asioista ja aiheeseen liittyvää kuvausta tietosuoja-asetuksen vaatimuksista. Esimerkiksi Käsittelyperiaatteiden huomioiminen -sivulla on kerrottu, mitä ovat tietosuoja-asetuksessa mainitut käsittelyperiaatteet ja mitä ne tarkoittavat. Geneeristen, organisaatioriippumattomien taustatieto-osuuksien lisäksi sivuille on tuotu organisaatiosidonnaista ohjeistusta. Esimerkiksi Rekisteröidyn oikeuksien huomioiminen -periaatesivulle on kuvattu, miten rekisteröidyn oikeudet Maanmittauslaitoksessa tänä päivänä toteutetaan, ja Arkaluonteisten henkilötietojen tunnistaminen -periaatesivulle on kirjoitettu turvakiellon ja yhteystietojen salassapitopäätöksen huomioimisesta. Kunkin sivun loppuun on liitetty tai tullaan myöhemmin liittämään viittauksia sekä Maanmittauslaitoksen sisäiseen dokumentaatioon että valtionhallinnon yleiseen ohjeistukseen liittyen aina kulloisenkin sivun aiheeseen.



Kuva 5.1: Maanmittauslaitokselle tutkimuksen yhteydessä toteutetun tietosuojaohjeistuksen sivurakenne

Tietosuojavaatimukset-sivulle on kerätty kaikki tutkielmassa tietosuoja-asetuksesta ja muusta henkilötietojen käsittelyä ohjaavasta lainsäädännöstä poimitut sovelluskehitykseen vaikuttavat vaatimukset (toive T9). Maanmittauslaitoksella vaatimuksia on yhteensä 97 kappaletta: luetteloon lisättiin Maanmittauslaitoksen erityistarpeista johtuen yksi uusi vaatimus liittyen yhteystietojen salassapitopäätökseen. Vaatimukset on järjestetty kappaleen 3 jaottelun mukaisesti yhdeksään eri kategoriaan. Jokaisella Tietosuojaperiaatteet-sivulla on siis vastinpari Tietosuojavaatimukset-sivun vaatimustaulukoissa. Vaatimukset on kirjattu vaatimustaulukkoon numeroituna samoin kuin tutkielmassa, ja kuhunkin vaatimukseen on merkitty, mihin TOGAFin ADM-mallin mukaisiin kokonaisarkkitehtuurin kehittämisvaiheisiin se liittyy. Kullekin vaatimukselle on lisäksi varattu tila huomautustekstille. Mikäli vaatimus ei ole relevantti Maanmittauslaitokselle tai sen käsittelyyn liittyy jotain erityistä huomioitavaa, on se merkitty tähän. Taulukon otsikkoon on liitetty linkki vastaavalle Tietosuojaperiaatteet-sivulle, ja kunkin sovellusarkkitehtuurivaiheen sarakeotsikosta pääsee siirtymään suoraan kyseisen vaiheen omalle sivulle.

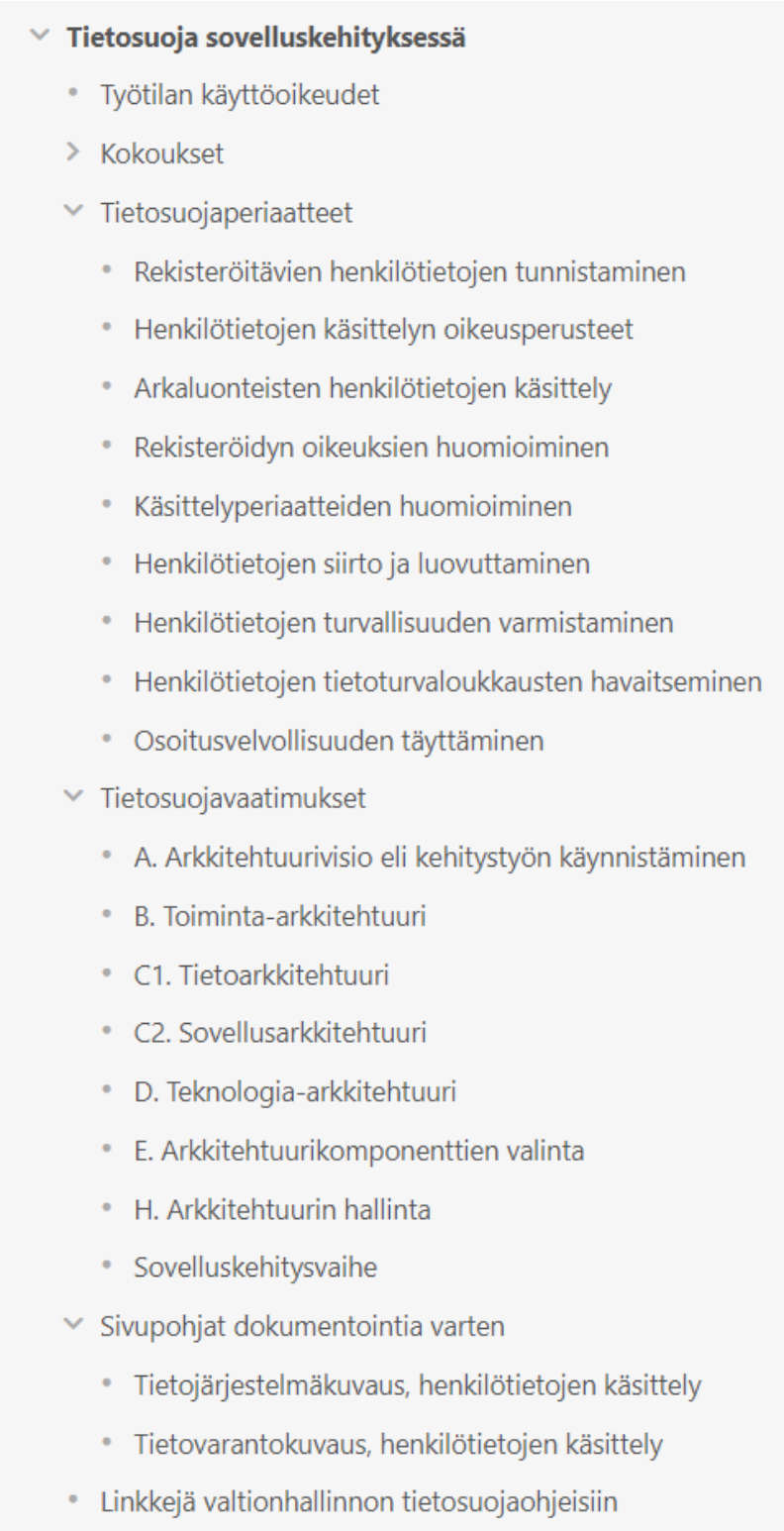
ADM-vaiheiden mukaiset vaihekohtaiset vaatimussivut (toive T2) on toteutettu kappaleessa 4.2 esitellyistä vaiheista A. Arkkitehtuurivisio, B. Toiminta-arkkitehtuuri, C1. Tietoarkkitehtuuri, C2. Sovellusarkkitehtuuri ja D. Teknologia-arkkitehtuuri. Lisäksi on toteutettu sivut E. Arkkitehtuurikomponenttien valinta (Mahdollisuudet ja ratkaisut) ja H.

Arkkitehtuurin hallinta kappaleessa 4.1 esitellyille vaiheille E ja H. Kullekin vaihekohtaiselle vaatimussivulle on tehty lyhyt kuvaus vaiheesta ja lueteltu ne tietosuojaan liittyvät asiat, joihin vaiheessa pitää ottaa kantaa. Tämän jälkeen vaiheessa käsiteltävät vaatimukset on ryhmitelty kysymysmuotoisten otsikoiden alle, ja muistilista-tyyppisesti (toive T3) kuvattu, minkälaisia toimenpiteitä niiden osalta tulee vaiheessa tehdä ja mitä taustamateriaaleja on käytettävissä. Kunkin vaatimuksen kohdalle on myös merkitty, mikä vaatimus on edeltänyt sitä ja mille vaatimukselle kyseinen vaatimus puolestaan tuottaa lähtötietoa. Vastuu eri vaiheiden toteuttamisesta on eri asiantuntijarooleilla (toive T10): toiminnan ja tietosuojan asiantuntijat ovat pääsääntöisesti vastuussa vaiheissa A ja B tehtävistä päätöksistä, kun taas arkkitehdit vastaavat vaiheiden C1, C2, D ja E toimenpiteistä. Vaihe H:n tekijöinä ovat tietosuoja-asiantuntijat ja sovelluskehittäjät.

Näiden kolmen pääsivutyypin lisäksi ohjeistoon toteutettiin sivupohjat henkilötietojen käsittelyn kuvaamiseksi tietojärjestelmissä ja tietovarannoissa sekä sivu, jolle kerättiin linkkejä valtionhallinnossa toteutettuun tietosuojamateriaaliin (toive T8). Maanmittauslaitokselle tämän tutkimuksen lopputuotoksena toteutetun **tietosuojaohjeistussivuston sisällysluettelo** on kokonaisuudessaan nähtävissä kuvassa 5.2.

Lyhyt esimerkki ohjeistuksen käyttötavasta:

1. On kyse henkilötietojen säilytysajan määrittelystä. Tietosuojavaatimukset-sivulta löytyy vaatimus 5.5 Rekisterinpitäjän on määriteltävä henkilötietojen säilytysaika mahdollisimman lyhyeksi. Vaatimus on luokiteltu otsikon Käsittelyperiaatteiden huomioiminen alle ja merkitty kuuluvaksi vaiheeseen B. Toiminta-arkkitehtuuri.
2. Taulukon otsikon kautta päästään siirtymään Tietosuojaperiaatteet-sivulle, jonka otsikko on sama kuin taulukolla eli Käsittelyperiaatteiden huomioiminen. Sivulta voidaan muun muassa lukea, että yksi henkilötietojen käsittelyperiaatteista on säilytyksen rajoittamisen periaate, jonka mukaan tietoja ei saa säilyttää yhtään kauempaa kuin on välttämätöntä, ja että henkilötietojen säilytysajan määrittelyssä tulee huomioida kansallisessa lainsäädännössä mahdollisesti olevat määräykset tietojen säilyttämisestä.
3. Kun periaatteet ovat selvät, voidaan palata Tietosuojavaatimukset-sivulle ja siirtyä sieltä tarkastelemaan vaiheessa B läpikäytäviä vaatimuksia. Vaihesivulta huomataan, että vaatimus 5.5 on merkitty kysymyksen Miten henkilötietojen käsittelyperiaatteet otetaan huomioon? alle. Toimenpiteissä todetaan, että henkilötietojen säilytysaika tulee päättää tässä vaiheessa selvittämällä lainsäädännölliset velvollisuudet sekä organisaation tarpeet tietojen säilytykselle. Taustatiedot-kohdassa on viittaus Tietosuojaperiaatteet-sivulle, ja siihen voidaan jatkossa kerätä muita viittauksia niin lakeihin kuin Maanmittauslaitoksen



Kuva 5.2: Maanmittauslaitoksen tietosuojaohjeistuksen sisällysluettelo (kuva Maanmittauslaitoksen Confluencen Tietosuoja sovelluskehityksessä -sivustolta)

sisäisiin ohjeisiin kuten esimerkiksi arkistonmuodostussuunnitelmaan, jossa määritellään asiakirjojen säilytysajat.
4. Vaatimustaulukosta nähdään myös, että vaatimusta 5.5 seuraa vaatimus 5.6, jonka osalta työ jatkuu vaiheessa C2 säilytysaikaan liittyvien toimintojen kuvaamisella sovellusarkkitehtuuriin. C2-vaiheessa säilytysaikaan liittyvät vaatimukset ovat kysymyksen Miten tiedot poistetaan säilytysajan jälkeen? alla. Toimenpiteissä luetellaan tarvittavat poistomenettelyn kuvaukset: tietojen poistosta on kuvattava poistofrekvenssi, tietojen sijainnit ja kunkin sijainnin säilytysaika, poistettavat tiedot ja poistomenetelmä, arkistointimenetelmä ja poistojen lokittaminen. Taustatietoina on tässä vaiheessa lokienhallinnan dokumentaatio.

Esimerkkiin liittyvät ohjesivut on tulostettu liitteeseen B.

ADM-vaiheisiin kiinnitettyjen vaihesivujen lisäksi on toteutettu Sovelluskehitysvaihe-sivu, jolle vaatimukset on ryhmitelty sen mukaan, mihin sovelluskehityksen kohteena olevaan komponenttiin ne kuuluvat. Tälle sivulle on koostettu muistilistat sovelluskehittäjille (toive T10). Vaatimuksia on tässä vaiheessa vielä jäljellä 69 kappaletta. Sivulla on huomioitu kappaleessa 4.2 mainitut kaksi vaatimusta, jotka eivät ole olleet käsittelyssä ennen sovelluskehitysvaihetta: vaatimukset 8.2 ja 8.7 liittyen tietoturvatestaukseen ja normaalista poikkeavien hakujen havaitsemiseen. Vaatimusten ja toimenpiteiden ryhmittelyssä on käytetty Maanmittauslaitoksen teknologiakäsikirjan [22] mukaista ryhmittelyä haastattelussa ehdotetun mukaisesti:

- Yhteiset tukipalvelut: Käyttövaltuushallinta, Lokienhallinta, Varmistuspalvelu, Valvontajärjestelmät
- ICT-infrastruktuuri: Ympäristöt, Tietokannat
- Sovellusarkkitehtuuri: Integraatioarkkitehtuuri
- Sovelluskehitys: Käyttöliittymä, Tulosteet ja tiedonluovutukset, Tietosisältö, Sovelluslogiikka, Sovellusten testaus

Kunkin vaatimuksen kohdalle on merkitty käsittelytoimenpide, joka sovelluskehitysvaiheessa sen suhteen odotetaan tehtäväksi. Jos sama käsittelytoimenpide koskee useampaa vaatimusta, on ne liitetty taulukossa yhteen. Esimerkissä C2-vaiheessa käsitelty vaatimus 5.6 löytyy Sovelluskehitysvaihe-sivulta otsikon Sovelluslogiikka alta, ja siihen on liitetty vaatimus 5.11, joka liittyy henkilötietojen minimointiin erityisissä käsittelytarkoituksissa.

Näille vaatimuksille on kirjattu käsittelyksi poistoajon toteuttaminen ja keinoiksi fyysinen poisto, anonymisointi, pseudonymisointi, tiedon maskaaminen ja päällekirjoittaminen.

Sovelluskehitysvaiheen tietosuojaohje on esitetty liitteessä C.

Haastatteluissa mainittiin erityisesti odotukset riskienarvioinnin ohjeistamiseen. Maanmittauslaitoksessa riskienarvioinnista jo olemassa olevat ohjeet on nyt liitetty Henkilötietojen turvallisuuden varmistaminen -periaatesivulle, jonne on viittaus kaikista niistä vaiheista, joissa riskienarviointia tulee tehdä (toive T6). Samoin Maanmittauslaitoksen lokienhallintaan ja käyttövaltuushallintaan liittyvä ohjeistus on nyt linkitetty C2-, E- ja Sovelluskehitysvaiheiden sivuille.

Varsinaisen tietosuojaohjeistuksen lisäksi rakenteeseen on toteutettu sivupohjat henkilötietojen käsittelyn kuvaamiselle sekä tietojärjestelmän että tietovarannon näkökulmasta. Sivupohjien ideana on, että sovelluskehittäjät voivat kopioida ne varsinaisen tietojärjestelmädokumentaation joukkoon täydennettäväksi tarpeen mukaan. Tarkoituksena on auttaa sovelluskehittäjiä dokumentoimaan oikeat ja riittävät asiat henkilörekistereiden käytöstä.

Viimeiseksi tietosuojaohjeistusrunkoon on lisätty sivu viittausten keräämiseksi keskeisiin suosituksiin ja valtionhallinnon ohjeisiin.

5.4 Tietosuojaohjeistuksen arviointi

Tietosuojaohjeistuksen runkosivustosta lähetettiin kommentointipyyntö yhteensä 33 Maanmittauslaitoksen tietosuoja-, it-, ja kokonaisarkkitehtuuriasiantuntijalle sekä kuudelle MITPAn esimiehelle. Vastauksia kommentointipyyntöön tuli määräaikaan mennessä 14 kappaletta.

Kaikki vastaajat olivat tyytyväisiä siitä, että tietosuoja-asetus on ohjeistuksen avulla tehty näkyväksi ja että ohjeistuksen kieli oli selkeää ja helppotajuista. Erittäin tärkeänä pidettiin sitä, että nyt kaikki tietosuojaan liittyvät sovelluskehitysohjeet voidaan jatkossa kerätä keskitetysti yhteen paikkaan, jolloin tieto löytyy helposti ja on kaikkien tarvitsijoiden saatavilla. Ohjeiston rakennetta kiitettiin: sitä pidettiin loogisena, selkeänä ja helposti jalkautettavana, ja vaikutti siltä, että se kattaa sovelluskehittäjän tarpeet. Periaate-sivujen tekstit olivat hyvin ymmärrettäviä ja vaikuttivat varsin riittäviltä siihen, että sovelluskehittäjä saa tarvittavan taustoituksen eri tietosuojaan liittyvistä aihealueista.

Vaatimusten esittämistä vaiheistettuna TOGAF-kehyksen ADM-arkkitehtuuriprosessin

mukaisesti pidettiin erittäin tärkeänä asiana ja hyvänä ideana, koska se antoi selvän kuvan siitä, mitä sisäänrakennetun tietosuojan aspekteja pitää huomioida missäkin arkkitehtuurikehittämisen vaiheessa, missä järjestyksessä ne on hyvä ratkoa ja millä tasolla vaatimukseen pitää milloinkin vastata. Kuten eräs haastateltu vaiheistusta kuvasi: ”Elefantti on nyt palasina.” Myös vaatimusten ryhmittelyä vaiheiden sisällä pidettiin toimivana ratkaisuna, kuten myös vaatimuksien purkamista edelleen kysymyksiksi, joihin tulee etsiä vastaukset. Vaiheistuksesta todettiin, että se tuo konkretiaa sovelluskehityksen tietosuojatyöhön.

Kommenttien perusteella tehtiin pieniä korjailuja sivustolle. Periaatesivujen järjestystä muutettiin tutkielman kappaleessa 3 olevan luokittelun mukaiseksi. Muita rakenteellisia muutosehdotuksia ei sivuston osalta esitetty. Sisällöllisesti suurin puute oli Maanmittauslaitoksen näkökulmasta turhan niukasti korostettu turvakiellon tai yhteystietojen salassapitopäätöksen omaavien henkilöiden henkilötietojen käsittelyn huomioiminen ja rajoittaminen. Siksi muistutuksia arkaluonteisten tietojen ja varsinkin turvakieltojen ja salassapitopäätösten käsittelyn huomioimisesta lisättiin lähes kaikkien vaiheiden ohjeistuksiin. Toinen aihe, johon kaivattiin lisätarkennuksia, oli henkilötietojen tuotantodatan eli oikeiden henkilötietojen käyttö sovelluskehitysvaiheessa toteutettavissa kehitys- ja testausympäristöissä. Siitä johtuen lisättiin teknologia-arkkitehtuuri- ja sovelluskehitysvaiheisiin toimenpiteitä, jotka liittyvät testi- ja kehitysympäristöjen käyttöön annettavan henkilödatan muokkaamiseen pseudonymisoinnin tai sotkemisalgoritmin avulla, sekä huomio siitä, että mikäli näissä ympäristöissä kuitenkin käytetään tuotantodataa, tulee se huomioida sekä henkilötietojen poistomenettelyissä että ympäristöjen käyttövaltuuksissa. Lisäksi täsmennettiin varmistuksista palauttamiseen mahdollisesti liittyvää henkilötietojen poistotarvetta ja lisättiin linkkejä jo olemassa olevaan ohjeistukseen sekä Maanmittauslaitoksen tietosuojaselosteisiin.

Muilta osin saadut kommentit olivat ohjeiston käytön ja sisällön pohdintaa. Terminologiaan liittyen eräs vastaaja pohdiskeli periaate-termin käyttöä: nyt ohjeistossa on tietosuojaperiaatteita, henkilötietojen käsittelyperiaatteita ja sisäänrakennetun tietosuojan periaatteita. Termin käyttö täsmentynee myöhemmin asian jalkautuessa paremmin organisaatioon. Sisäänrakennetusta tietosuojasta todettiin myös, että se ei ole itsenäinen saareke, vaan sillä on liittymänsä niin tietoturvaan, jatkuvuudenhallintaan, käyttövaltuushallintaan ja lokienhallintaan kuin myös hankinta- ja sopimusasioihin. Kyseessä on siis laajempi kokonaisuus kuin miltä se ensiajattelemalta kuulostaa. Eräs vastannut totesikin suorastaan hengästyneensä sisäänrakennetun tietosuojan vaatimusten määrästä ja arviostaan liittyen niiden aiheuttamaan työmäärään sovelluskehityksessä.

Eräs asiantuntija kertoi, että vaikutustenarviointiin liittyen odotetaan EU:n tietosuojaneuvostolta linjauksia korkean riskin arviointiin. Kun näitä linjauksia saadaan, tulevat ne täsmentämään myös nyt kehitettyä ohjeistusta riskien- ja vaikutustenarvioinnin osalta.

Saatujen kommenttien perusteella voidaan todeta, että Maanmittauslaitokselle toteutettu sovelluskehittäjien tietosuojaohjeistuksen runko vaikuttaa tarkoitukseensa soveltuvalta, ja että sen ympärille on mahdollista rakentaa kattava ohjeistus sille, miten sisäänrakennetun tietosuojan periaatteita toteutetaan Maanmittauslaitoksen sovelluskehityksessä. Toki kommentoijien määrä jäi toivottua pienemmäksi vastausprosentin ollessa vain 36%, mikä voi tarkoittaa sitä, että vasta ohjeiston käytön alkaessa ilmenee todellinen mielipide sen käytettävyydestä. Nyt saadut kommentit olivat kuitenkin niin positiivisia, että voidaan arvioida ohjeistuksen löytävän käyttäjänsä. Haastattelujen perusteella saadut toiveet olivat osittain ristiriidassa keskenään: toiset haastatelluista toivoivat väljää ohjeistusta, mikä mahdollistaisi soveltamisen ja oman päätöksenteon, toiset toivoivat hyvinkin tarkkaa ohjeistusta, jotta ei tulkinnanvaraisuutta syntyisi. Nähtäväksi jää, vastaako nyt luotu ohjeistus lopulta käyttäjiensä vaatimuksia.

Ohjesivustoa tulee ehdottomasti edelleen jatkokehittää. Haastatteluissa kerätyistä tarpeista monet jäivät kokonaan toteuttamatta joko aikatauluhaasteiden tai linjausten puuttumisen vuoksi. Jotta sisäänrakennetun tietosuojan toteuttamisen vaatima työmäärä jäisi kohtuulliseksi, tulee ohjeistuksessa pyrkiä esittämään ratkaisuja, jotka ovat riittävän geneerisiä käytettäväksi kaikissa palveluissa, mutta toisaalta riittävän yksityiskohtaisia, jotta asiantuntijoiden ei tarvitse keksiä toteutustapaa joka kerta uudelleen. Parhaiden käytäntöjen ja ideoiden jakamista niin Maanmittauslaitoksen sovelluskehitystiimien kuin valtionhallinnon toimijoiden kesken tulee jatkaa ja lisätä, ja kerätä niistä soveltuvimmat myös tähän ohjeistoon.

6 Pohdinta

Tämän tutkielman tavoitteena oli löytää vastauksia kahteen tutkimuskysymykseen: Minkälaisia vaatimuksia EU:n yleinen tietosuoja-asetus asettaa sovelluskehitykselle ja minkälaista ohjeistusta sovelluskehittäjät tarvitsevat sisäänrakennetun tietosuojan huomioimiseksi sovelluskehityksessä. Tässä kappaleessa käydään läpi tutkielman tekemisen aikana tehtyjä havaintoja liittyen tutkimuskysymyksiin. Koska tutkielman lopputuotos, sovelluskehityksen tietosuojaohjeistuksen runko, toteutettiin Maanmittauslaitokselle, arvioidaan tutkimuskysymyksiä ja tutkielman vastausta niihin Maanmittauslaitoksen näkökulmasta.

6.1 TK1: Vaatimukset sovelluskehitykselle

Tietosuoja-asetus on varsin pitkä ja monimutkainen asetus. Henkilötietojen käsittelyssä on huomioitava näkökulmia hyvin laajalla sektorilla: periaatteiden, rekisteröidyn oikeuksien ja rekisterinpitäjän velvollisuuksien lisäksi se asettaa velvoitteita ja rajoitteita henkilötietojen käsittelylle EU:n ulkopuolella, valvontaviranomaisten toimivallalle, viranomaisten yhteistyölle ja yhdenmukaisuudelle EU:n sisällä, oikeussuojakeinoille ja seuraamuksille, tietojenkäsittelyyn liittyville erikoistilanteille sekä asetuksen suhteelle muihin lakeihin. Tämän seurauksena tietosuojasta on lopulta kirjoitettu monipolvinen asetus, joka sisältää 11 lukua ja 99 artiklaa, ja joka paperille tulostettuna on peräti 107 sivun mittainen. Koska henkilötietojen käsittelyä tehdään tänä päivänä arvatenkin pääasiassa tietoteknisin keinoin, ei ole yllättävää, että asetus sisältää hyvin paljon vaatimuksia nimenomaan sovelluskehitykselle.

Tietosuoja-asetuksessa esille nostettu Privacy by Design -käsite toimii mielestäni vahvana motiivina tämän tutkimuksen työlle. Se asettaa sovelluskehitykselle velvoitteen huomioida tietosuojavaatimukset sovelluskehityksessä sen käynnistämisestä lopputuotoksen käyttöönottoon asti. Sisäänrakennetun ja oletusarvoisen tietosuojan, kuten käsitteitä Privacy by Design ja Privacy by Default asetuksessa kutsutaan, ero ei selvinnyt tietosuoja-asetuksen määritelmistä erityisen hyvin, vaan niiden ymmärtäminen vaati perehtymistä Ann Cavoukianin lanseeraamiin Privacy by Design -periaatteisiin [1]. Periaatteet ovat olleet aikaansa edellä: on melko yllättävää, että ne on luotu jo 25 vuotta sitten, jol-

loin tietotekninen maailma oli huomattavan paljon suppeampi ja hitaampi kuin tänä päivänä. Ne ovat kuitenkin kestäneet aikaa hyvin ja ovat edelleen käyttökelpoisia, kun puhutaan henkilötietojen suojaamisen periaatteista. On huomattava, että Privacy by Design -periaatteet eivät lähtökohtaisesti koske vain tietojärjestelmäkehitystä, vaan myös toiminta-arkkitehtuurin muutoksia kuten prosessien kehittämistä. Sisäänrakennettu ja oletusarvoinen tietosuoja kuuluvat Cavoukianin seitsemän Privacy by Design -periaatteen joukkoon. Niiden erottaminen toisistaan vaati hieman pohdintaa ja sisäistämistä. Tulkitsin niitä siten, että sisäänrakennettu tietosuoja toteutetaan organisaation kokonaisarkkitehtuuria kehittämällä, jotta oletusarvoinen tietosuoja on jo olemassa siinä vaiheessa, kun kyseinen arkkitehtuurimuutos on saatu käyttöön – sisäänrakennettu tietosuoja on ne keinot, joiden avulla tietosuojaa toteutetaan, oletusarvoinen tietosuoja puolestaan luottamus siihen, että kyseisiä keinoja on riittävästi käytetty. Tämän tulkinnan mukaisesti keskityin tutkielmassa nimenomaisesti sisäänrakennetun tietosuojan periaatteeseen.

Tutkielman ensimmäiseksi tutkimusongelmaksi olin valinnut sovelluskehitykseen vaikuttavien vaatimusten löytämisen tietosuoja-asetuksesta. Koska henkilötietojen suojaa säätelee myös muun muassa tietosuojalaki ja julkisuuslaki, sisällytin nämäkin vaatimustarkasteluun. Tämä osoittautui työn kuluessa melko laajaksi rajaukseksi. Sovelluskehitykseen vaikuttavia sisäänrakennetun tietosuojan vaatimuksia laeista kertyi lopulta 96 kappaletta. Havaitsemieni vaatimusten osalta tein subjektiivista arviointia sen suhteen, mitkä vaatimuksista olivat todellisuudessa sovelluskehitykseen ja sovellusarkkitehtuuriin vaikuttavia vaatimuksia, jotta saatoin keskittyä vain tutkielman kannalta olennaiseen sisältöön. Arvioin, että nyt koostettu vaatimusluettelo tulee täsmentymään, kun sitä ryhdytään hyödyntämään sovelluskehitysprojekteissa. Vaatimusluetteloa ei olekaan tarkoitettu muuttumattomaksi, vaan sen soveltaminen ja muokkaaminen organisaation toimintaa paremmin tukemaan on enemmän kuin suotavaa. Toteutin vaatimusluettelon geneeriseksi ratkaisuksi jättämällä huomioimatta Maanmittauslaitoksen viranomaisroolista tulevia erityispiirteitä, joten se on hyödynnettävissä kaikissa muissakin organisaatioissa, joissa nähdään tarvetta määritellä sisäänrakennetun tietosuojan vaatimuksia sovelluskehitykselle.

Asetuksen sisältämien vaatimusten luokittelu oli välttämätöntä, jotta ne oli mahdollista järjestää tutkielman näkökulmasta järkeviksi kokonaisuuksiksi. Asetuksen luvut vastaavat osittain nyt tehtyä luokittelua, mutta ne eivät etene sovelluskehityksen näkökulmasta loogisessa järjestyksessä. Siksi päädyin kappaleessa 3 esiteltyyn luokitteluun ja luokittelujärjestykseen. Järjestys perustuu siihen kokemukseen, mikä allekirjoittaneella on organisaatioiden projektityö- ja systeemityömenetelmistä. Tässä tapauksessa on ensimmäiseksi

määriteltävä perusteet tietosuojatoiminnoille: arvioitava, käsitelläänkö henkilötietoja sekä millä perusteella ja missä tarkoituksessa niitä käsillään. Vasta tämän jälkeen on järkevää alkaa suunnitella toiminnallisia ja tietoteknisiä muutoksia arkkitehtuuriin: mitä henkilötietoja käsitellään ja miten. Lopulta arvioidaan, miten tiedot turvataan riittävän hyvin ja miten täytetään osoitusvelvollisuuden vaatimukset. Tietosuoja-asetuksen sisällön esittelystä teki haastavaa sen laajahko sisältö sekä lakiteksteille tyypilliset pitkät luettelot. Koska sovelluskehitykseen vaikuttavia artikloja ja niissä olevia yksittäisiä vaatimuksia löytyi runsaasti, ei niiden muotoilu luettavaksi ja ymmärrettäväksi tutkielmatekstiksi ollut yksinkertaista, ja tutkielmasta tulikin varsin pitkä. En kokenut kuitenkaan mahdolliseksi jättää mitään nyt mukana olevia näkökulmia pois tutkielmasta, koska se olisi karsinut myös relevantteja vaatimuksia pois vaatimusluettelosta.

Jo Maanmittauslaitoksen ensimmäisessä tietosuojaprojektissa todettiin, että tietosuoja-asetuksesta sovelluskehitykselle tulevat vaatimukset tulee liittää sovelluskehitysprojektin vaiheisiin niin, että ne voidaan täyttää oikea-aikaisesti ja oikeassa järjestyksessä. Projektissa tätä hahmoteltiin tehtäväksi perinteisen vesiputousmallin systeemityövaiheiden mukaisesti, mutta siihen ei löytynyt tuolloin tyydyttävää ratkaisua: lähes kaikki silloin esiin nostetut seikat (vaatimuksiksi niitä ei voinut vielä kutsua) asettuivat lopulta tehtäväksi joko jo ennen projektia tai sen määrittelyvaiheeseen. Näin aikataulullinen priorisointi eri vaatimusten kesken tuntuikin hankalalta ja työ jäi kesken. Kaksi vuotta kestänyt perehtymisjaksoni tutkielman aiheeseen kuitenkin selkiytti ajatuksia: julkishallinnon JHS 179 -kokonaisarkkitehtuurimenetelmän [14] tuntemus herätti ajatuksen vaatimusten liittämisestä kokonaisarkkitehtuurikerroksiin, ja tutustuminen TOGAF-kokonaisarkkitehtuurikehykseen [24] ja varsinkin sen ADM-kehittämisprosessiin auttoi löytämään tutkielmaan mielestäni hyvin soveltuvan viitekehyksen sisäänrakennetun tietosuojan vaatimusten järjestämiseksi niin, että tarvittavat päätökset ja määritykset tietosuojan implementoimiseksi kehitettävään tietojärjestelmään saadaan organisaatiossa tehtyä vaiheistetusti jo ennen varsinaisen sovelluskehitysprojektin käynnistymistä. Sillä vaikka sovelluskehitystä tehdäänkin nykyään lähinnä ketterillä menetelmillä, ei tarve vanhanaikaisen vesiputousmallin määrittely- ja suunnitteluvaiheille ole kadonnut minnekään. Tässä tutkielmassa ehdotetaan, että henkilötietojen tietosuojaan liittyvä määrittely- ja suunnittelutyö tehdäänkin kokonaisarkkitehtuurin kehittämistyönä jo ennen varsinaista sovelluskehitystä. Maanmittauslaitoksessa tämä työ toteutetaan usein suunnitteluprojektina, joka edeltää varsinaista toteutusprojektia.

Tietosuoja-asetuksesta poimittujen sisäänrakennetun tietosuojan vaatimusten kiin-

nittämisen TOGAF-kokonaisarkkitehtuurikehyksen ADM-kehittämisprosessin vaiheisiin antoi siis vaatimuksille ajallisen järjestyksen. Vaiheistamisen yhteydessä havaitsin, että noin kolmasosaa 96 vaatimuksesta joudutaan käsittelemään kahdessa tai useammassa arkkitehtuurikehittämisen vaiheessa. Tämän lisäksi vajaa kaksi kolmannesta vaatimuksista on sovelluskehitysvaiheessa huomioitavia vaatimuksia. Vaatimusten kiinnittämisestä TOGAF-in mukaisiin vaiheisiin oli kahdenlaista hyötyä tutkimustyölle. Tein vaatimusten vaiheistamista iteroiden, tutkimustyön edistyessä niitä useamman kerran tarkastellen, ja havaitsin siinä yhteydessä muutostarpeita myös vaatimuksiin, jotta pystyin perustelemaan niille valitun vaiheistuksen. Nämä muutokset olivat tarkennuksia, mutta myös uusien vaatimusten luomista, jotta yksittäisistä vaatimuksista tuli vaiheisiin sopivia. Samalla vaatimusten järkevyys ja riittävyys tuli ristiintarkastettua: ne etenevät nyt loogisesti ja kattavasti. Tehty vaiheistus loi hyvän pohjan tutkielman lopputuotoksen eli tietosuoja-ohjeistuksen tekemiselle: käytännössä tässä vaiheessa tekemäni vaatimus-vaihe-matriisi oli mahdollista ottaa lähes sellaisenaan osaksi tietosuojaohjeistusta, sen lähtökohdaksi. Myös tässä yhteydessä tapahtui iteraatiota, koska ohjeiden kirjoittaminen vaikutti niin vaatimuksiin kuin niiden vaiheistukseen. Jotta vaiheistettu vaatimusluettelo olisi hyödynnettävissä tarvittaessa myös muissa organisaatioissa kuin Maanmittauslaitoksessa, tein vaiheistuksesta mahdollisimman geneerisen ratkaisun. Toki vaatimusten kiinnittäminen eri arkkitehtuurikehittämisen vaiheisiin on tehty subjektiivisella näkemyksellä omaan kokemukseen perustuen, joten on todennäköistä, että niitä on organisaatiokohtaisesti jonkin verran sovellettava.

Tekemääni tutkimustulosta on tarkoitus hyödyntää Maanmittauslaitoksen tulevissa sovelluskehityshankkeissa. Työn ansiosta jokaisen projektin tai hankkeen ei tarvitse erikseen tutustua tietosuoja-asetukseen ja tulkita sen vaatimuksia, vaan projektit voivat valita vaatimusluettelosta kulloiseenkin tarpeeseen soveltuvat tietosuojavaatimukset liitettäväksi projektisuunnitelmaan. Koska vaatimukset on jo valmiiksi vaiheistettu, helpottaa se tehtävien järjestämistä projektisuunnitelmaan niin, että tarvittavat päätökset saadaan oikea-aikaisesti. Tämä vähentää omalta osaltaan projektin valmistelutyöhön kuluvaa aikaa ja henkilötyötä ja parantaa todennäköisyyttä ottaa sovelluskehityksessä huomioon kaikki tarvittavat sisäänrakennetun tietosuojan vaatimukset. Lisäksi vaatimusten avulla on mahdollista havaita tarpeita yhteiskäyttöisille ratkaisukomponenteille, joiden toteuttamista tietojärjestelmien yhteiseen käyttöön soveltuviksi kannattaa arkkitehtuurityössä harkita. Näitä ratkaisukomponentteja voivat olla esimerkiksi rekisteröidyn oikeuksien huomioiminen ja niihin kohdistuvien toimintojen toteuttaminen tietojärjestelmiin. Kuten todettu, vaatimusluettelo ei varmasti ole täydellinen, vaan se toivottavasti muotoutuu käytön

myötä vastaamaan paremmin tarkoitustaan. Uhkana työni validiudelle on lain kirjaimen tulkinta: olenko arvioinut tutkielmassa lakiin kirjattuja vaatimuksia oikein. Virhetulkinnan mahdollisuutta osaltaan pienentänee se, että osallistuminen Maanmittauslaitoksen tietosuojaprojekteihin on mahdollistanut tietosuoja-asetuksen sisältöön tutustumisen organisaation lakiasiantuntijoiden myötävaikutuksella.

Toiveenani oli ehtiä paneutua myös tietosuojaa tukeviin tietoturvakäytäntöihin, mutta siihen ei ollut tutkimuksen aikana resursseja. Tietosuojaan liittyvät tietoturvatoimenpiteet ovat potentiaalinen ehdokas uudelle tutkimukselle. Arvatenkin näitä tutkimuksia on jo tehty, mutta aihe on monipuolinen ja ajankohtainen nykypäivänä esiintyvien tietoturvallisuusuhkien vuoksi. Monet toimenpiteistä kuten tietojen salaaminen siirrettäessä niitä verkossa sekä keskitetty käyttövaltuushallinta ja lokienhallinta ovat jo yleisesti organisaatioiden käytössä, mutta niiden lisäksi löytyy vähemmän esiteltyjä menetelmiä kuten pseudonymisointi ja anonymisointi, jotka ansaitsisivat tulla periaatteiltaan ja sovellutuksiltaan paremmin tunnetuiksi. Syystä tai toisesta anonymisointia ei ole tietosuoja-asetuksessa lainkaan mainittu tietosuojaa parantavana käytänteenä. Liekö syy siinä, ettei anonymisoitu tieto ole enää henkilötietoa. Se on kuitenkin hyvin relevantti tapa poistaa henkilötietoja säilytysajan päätyttyä, rekisteröidyn peruuttaessa suostumuksensa rekisteröintiin tai hänen käyttäessään oikeuttaan pyytää tietojen poistoa, mikäli on kuitenkin edelleen tarvetta säilyttää tieto siitä, että kyseinen rekisteröintitapahtuma on joskus tapahtunut. Potentiaalisiin tietoturvamenetelmien tutkimuskohteisiin kuuluvat myös PETs-teknologiat [3], joita tutkielmassa vain lyhyesti sivuttiin.

Tiedonhallintalain vaikutukset julkishallinnon tietosuojadokumentaation tuottamiseen on vielä avoin kysymys. Laki on tullut voimaan kuluvan vuoden alusta, ja sen toimeenpanoon on aikaa vuoden loppuun asti. Lakitekstiin kirjatut vaatimukset organisaation kokonaisarkkitehtuurin systemaattiselle dokumentoinnille ovat kuitenkin hyvin laajat ja tarvitsevat toteutuakseen soveltamisohjeita, jotta julkishallinnon toimijat kykenevät ymmärtämään ne edes jotakuinkin samalla tavalla. Valtionhallinnon organisaatioissa on käynnistynyt lain velvoitteiden täyttämispyrkimykset, mutta työ pääsee käynnistymään kunnolla vasta nyt loppukeväästä tiedonhallintalautakunnan (https://vm.fi/tiedonhallintalautakunta) julkaistua suosituksensa tiedonhallintamallista juurikin tätä kirjoittaessani [28]. Tiedonhallintalaki ja sen vaikutukset julkishallinnon toimintaan olisi myös hyvin mielenkiintoinen uusi tutkimuskohde.

6.2 TK2: Vaatimukset ohjeistukselle

”Privacy by Design -periaate ei ole kaikissa tapauksissa riittävä varmistamaan, että tarvittavat teknologiset tietosuojaperiaatteet on kunnolla sisällytetty tietojenkäsittelyyn. Joskus tarvitaan konkreettisempi ’hands on approach’.” [3]

Jo Maanmittauslaitoksen tietosuojaprojektien aikaan kävi selväksi, että organisaation sovelluskehittäjät tarvitsevat ja odottavat saavansa täsmällistä sovelluskehitysohjeistusta tietosuojan huomioimiseksi tietojärjestelmissä. Siksi tutkielman toinen tutkimuskysymys kuuluikin: Minkälaista ohjeistusta sovelluskehittäjät tarvitsevat sisäänrakennetun tietosuojan huomioimiseksi sovelluskehityksessä? Tätä kysymystä ratkaisemaan kutsuin 19 Maanmittauslaitoksen asiantuntijaa, jotka kaikki ovat jossain roolissa tekemisissä sovelluskehityksen kanssa: varsinaisina sovelluskehittäjinä, arkkitehteinä tai teknisinä asiantuntijoina. Lähetin haastatelluille etukäteen listan kysymyksistä (kappaleessa 5.2) sekä liitteenä tietosuojaan liittyviä käsitteitä ja tietoturvatoimenpide-ehdotuksia lähinnä muistuttamaan siitä, mitä kaikkea tietosuoja näkökulmana sisältää. Kukin 2–3 asiantuntijan haastattelu kesti tunnin.

Haastattelun lopputulos ei ollut yllättävä: ohjeistusta tarvitaan, sen halutaan olevan keskistetyssä paikassa ja sen pitää olla napakkaa ja selkeälukuista, ei proosaa. Haastatteluilla oli kuitenkin suuri merkitys sille, minkälaiseksi ohjeisto alkoi keskustelun jälkeen muotoutua. Haastatteluissa esitetyistä ideoista varsinkin kolme oli sellaisia, jotka vaikuttivat visioon ohjeiden muodosta: ennakoitavissa ollut idea vaatimusluettelon hyödyntämisestä projektien käyttöön, erinomainen idea valmiista tietosuojavaatimusten testitapausjoukosta Maanmittauslaitoksessa testauksen tukena jo käytössä olevaan Atlassianin Jira-tehtävienhallintatuotteeseen, sekä toive eri kohderyhmille – substanssiasiantuntijoille, arkkitehdeille ja sovelluskehittäjille – tarkoitetuista ohjeistuksista. Myös toiveet linkeistä keskeisiin ohjeisiin ja suosituksiin sekä selvä epätietoisuus Maanmittauslaitoksessa jo olemassa olevasta ohjeistuksesta liittyen teknologiaratkaisujen käyttöön sovelluskehityksen rakennuskomponentteina olivat ajatuksina esillä, kun suunnittelin ohjesivuja Confluenceen.

Tutkimuskysymykseen tutkimus vastasi hyvin, kun ohjeistuksen kohteena oli Maanmittauslaitos. Koen, että haastateltavana oli hyvä otos Maanmittauslaitoksen asiantuntijoita, joilta sain hyvin tietoa siitä, minkälaista ohjeistusta sovelluskehittäjät sisäänrakennetusta tietosuojasta kaipaavat. Toiveet olivat toki osittain ristiriidassa keskenään: toiset toivoivat väljää ohjeistusta, mikä mahdollistaisi soveltamisen ja oman päätöksenteon, toiset toivoivat hyvinkin tarkkaa ohjeistusta, jotta ei tulkinnanvaraisuutta syntyisi. Tämä selit-

tyy kyseisten asiantuntijoiden tehtävien heterogeenisyydellä ja myös heidän eriasteisella kokemuksellaan tietosuojatehtävistä. Selvästi tietosuojan vaatimukset olivat kuitenkin sen verran epäselviä, että ohjeistusta todellakin tarvitaan, jotta asiat ymmärretään samalla tavalla.

Ohjeistuksesta on nyt tutkimuksen päättyessä olemassa ensimmäinen versio. Varsin paljon toiveita jäi kuitenkin vielä toteutettavaksi tutkimuksen jälkeen. Idea valmiista testitapausjoukosta on sovittu toteutettavaksi mahdollisimman pian, ja riskienarviointiin olemme Maanmittauslaitoksen asiantuntijan kanssa jo ideoineet tietosuojan itsearviointitarkistuslistaa, jonka avulla projektit voivat eri vaiheissaan alustavasti itse tarkistaa, onko aihetta lisätoimenpiteille. Myös erityislainsäädännön kriteerien ja valtionhallinnon linkkien selvittäminen on mahdollista toteuttaa melko nopeasti. Käyttövaltuushallintaan ja lokienhallintaan liittyvät toiveet lisäohjeistuksesta on helppo siirtää niistä vastaavien asiantuntijoiden tehtäväksi.

Jäljelle jää joukko toiveita, joiden täyttäminen edellyttää toimia Maanmittauslaitoksen sovelluskehityksen vastuuhenkilöiltä. Toiveiden toteuttamiseksi tarvitaan päätöksiä muun muassa sovellusarkkitehtuuriratkaisuista ja sovellusarkkitehtuurin kehittämisen organisoinnista. Sisäänrakennetun tietosuojan toteuttamisen valvonta vaatii katselmointimenettelyt ja tekijät. Kokonaisarkkitehtuurikuvausten kuten esimerkiksi loogisten ja fyysisten tietovirtakaavioiden tekemiseen tarvitaan ohjeistusta ja mallikuvauksia organisaation kokonaisarkkitehdeiltä. Ohjeeseen arkaluonteisten henkilötietojen käsittelystä vaaditaan vankkaa näkemystä myös lakiasiantuntijoilta. Jotta tarvittavien sovelluskehitysohjeiden tekeminen onnistuisi, olisi työtä varten nimettävä työryhmä, joka alkaa koota yhteistä Maanmittauslaitoksen näkemystä siitä, miten tietosuojavaatimukset toteutetaan järjestelmiin samalla tavalla ja tarkkuudella. Toivomukseni onkin, että Maanmittauslaitos organisoi sovelluskehityksen tietosuojatyön nyt, kun siinä on saatu ensimmäinen ponnistus tehtyä ja ensimmäiset ohjeistukset toteutettua. Maanmittauslaitoksessa toimii arkkitehtuuriryhmä, joka pohtii lähinnä tietojärjestelmä- ja teknologia-arkkitehtuurien linjauksia. Jos sovelluskehitykseen liittyvä tietosuojatyön kehittäminen vastuutetaan kyseiselle ryhmälle, tarvitsee se tuekseen sovelluskehittäjien resursseja, jotta tarvittavat näkökulmat osataan huomioida riittävän hyvin toteutettavassa ohjeistossa.

Toivon, että tekemääni ohjeistoa osataan hyödyntää Maanmittauslaitoksessa ja että sitä myös kehitetään eteenpäin sitä mukaa, kun projekteissa löydetään hyviä käytäntöjä, jotka on syytä jakaa muillekin. Nyt ohjeistuksessa mainitut toimenpiteet eri vaatimusten toteuttamiseksi perustuvat allekirjoittaneen pitkään kokemukseen it-alalla. Toimenpiteet

ovat tällä hetkellä muistilistatyyppisiä, ja vastuu niiden toteuttamistavasta jää kokonaan sovelluskehittäjälle. Siksi ohjeistuksen olisi toivottavaa elää ja kehittyä sitä mukaa, kun siinä huomataan puutteita ja tarvetta tarkennuksille. Uskon, että nykyistä ohjerunkoa tullaan laajentamaan jatkossa lisäohjeistuksella, ja sivustosta rakentuu toimiva kokonaisuus niin Maanmittauslaitoksen sisäisten sovelluskehittäjien kuin myös ulkoisten toimittajien käyttöön. Koska työ oli mittatilaustyö Maanmittauslaitokselle, ei sen sisältö ole käyttöönotettavissa muissa organisaatioissa. Tutkielman liitteenä B on ohjeistoesimerkki, jota voi toki hyödyntää muiden organisaatioiden vastaavan ohjeiston ideoinnissa. On toki mahdollista, että tehty työ jää hyödyntämättä tai että se ei vastaakaan vielä varsin vajaavaisena niitä toiveita, joita siihen on asetettu. Saamani palautteen perusteella uskon kuitenkin, että tehdyn kaltaiselle tietosuojaohjeistolle on ollut tilausta ja että se vakiintuu Maanmittauslaitoksen sovelluskehityskäytänteiden joukkoon. Luotan myös siihen, että Maanmittauslaitos arvostaa tietosuojaohjeistustyötä ja nimeää tarvittavat resurssit sen jatkamiselle.

Mahdollisia tutkimusaiheita läheltä nyt tehdyn tutkimuksen aihepiiriä ovat tutkimus sovelluskehittäjien tietosuojaosaamisesta eri organisaatioissa sekä tutkimus parhaista käytännöistä sisäänrakennetun tietosuojan implementoimiseksi eri organisaatioiden sovelluskehitystyöhön.

6.3 Aiheeseen liittyvät muut tutkimukset

Tietosuoja-asetukseen liittyen on tehty runsaasti aiempia pro gradu -tutkimuksia suomalaisissa yliopistoissa. Tietojenkäsittelytieteen maisteriopintoihin liittyen on tehty kolme otsikkonsa perusteella lähelle tämän tutkielman aihetta osuvaa aiempaa tutkimustyötä, joita ei ollut käytettävissä sähköisessä muodossa: Joonas Jokiniemen Rekisterinpitäjää koskevat velvoitteet EU:n yleisen tietosuoja-asetuksen (GDPR) mukaan ja näiden velvoitteiden huomioiminen tietojärjestelmissä (2018, Tampereen yliopisto), Esapekka Kalliolan Yleinen tietosuoja-asetus: Sanktiot ja niiltä välttyminen (2019, Tampereen yliopisto) sekä Tuomas Ollin GDPR – Euroopan tietosuoja-asetuksen tietotekniset vaatimukset henkilötietojen käsittelijälle ja vaatimusten aiheuttamat muutokset kohdeyrityksen tietoaineistoturvallisuuden tasoon (2019, Vaasan yliopisto).

Kalle Hjerppen pro gradu -tutkielmassa Yleinen tietosuoja-asetus ja ohjelmistoarkkitehtuuri (2018, Turun yliopisto) [13] kirjoittaja on käsitellyt tietosuoja-asetusta ja sen vaikutuksia sovelluskehitykselle selvittäen, mitä vaatimuksia tietosuoja-asetus asettaa tie-

tojärjestelmille ja millainen ohjelmistoarkkitehtuuri tukisi tätä parhaiten. Kuten myös tässä tutkielmassa, on Hjerppe johtanut asetuksesta vaatimusmäärittelyn, joiden perusteella on hahmoteltu esimerkkiarkkitehtuuri, joka koostuu kuudesta tietosuojamoduulista. Hän on todennut, että vaatimusmäärittely on mahdollista tehdä ja arkkitehtuuri suunnitella etukäteen, koska asetuksen vaatimukset ovat stabiilit eikä niitä voi jättää huomioimatta. Hän on myös havainnut, että asetuksen sanamuodot jättävät runsaasti tulkinnan varaa, koska termin ”asianmukaiset toimenpiteet” määrittäminen jää kunkin organisaation omalle vastuulle. Hjerppe on löytänyt yhdeksän teknistä vaatimusta, joilla kullakin on 0–7 alavaatimusta. Vaatimuksista on johdettu kuusi käyttäjätarinaa, joissa kaikissa aktorina toimii rekisteröity. Tutkimuksen artefaktina on syntynyt kuvaus ratkaisuarkkitehtuurista kahdelle tutkimuskohteena olleelle yritykselle. Molempien pro gradu -tutkielmien lähtökohtana on ollut löytää yleiset vaatimukset sisäänrakennetulle tietosuojalle. Hjerppe on kuitenkin käsitellyt aihetta tietosuojaa toteuttavien, uudelleenkäytettävien arkkitehtuurikomponenttien näkökulmasta, kun taas oma tutkielmani on kuvannut vaatimusten käyttöä yksittäisen kehityshankkeen lähtökohdista osoitusvelvollisuuden täyttämiseen tähdäten. Hjerppen hahmottelema arkkitehtuuriratkaisu vaikuttaa toimivalta, ja siinä on huomioitu muun muassa pseudonymisointiprosessin toteuttava komponentti, jollaista tähän tutkimukseen haastatelluistakin pari toivoi määriteltäväksi myös Maanmittauslaitokselle.

Hjerppen tutkielman lisäksi ei löytynyt muita erityisesti vaatimusmäärittelyyn kohdistuvia tutkielmia, jotka olisivat käsitelleet tietosuoja-asetuksen vaatimuksia kokonaisuudessaan. Tyypillisesti tietosuoja-asetusta käsittelevät tutkimukset ovat kohdistuneet jollekin kapeammalle sektorille tietosuoja-asetuksen sisällössä.

Magnus Westerlund on tehnyt Åbo Akademille väitöskirjan aiheesta A study of EU data protection regulation and appropriate security for digital services and platforms (2018) [32]. Siinä hänen tavoitteenaan on ollut selvittää, miten tietosuoja-asetusta tulee tulkita niin sanottujen älykkäiden järjestelmien, joihin usein liittyy automaattisia päätöksentekoa ja profilointia, yhteydessä, mitä ovat tulevaisuuden ”riittävän tietoturvan” sovellutukset ja miten tietosuoja-asetus jatkossa ohjaa digitaalisten alustojen jatkuvaa kehittämistä. Väitöskirja keskittyy pitkältä teknologia-arkkitehtuurikerroksen ratkaisujen selvittämiseen, ja käsittelee muun muassa hajautettuja, esimerkiksi lohkoketjuihin perustuvia tietojärjestelmiä, joissa henkilötieto voi olla tietosuoja-asetuksen hengen mukaisesti hyvin pitkälle pseudonymisoitua, mutta jonka osalta rekisteröidyn oikeuksien täyttäminen voi olla haastavaa, koska tiedon omistajuus ei välttämättä ole itsestään selvää. Tämän tut-

kielman kannalta mielenkiintoisinta oli pohdinta siitä, miten rekisteröidyllä ei ole todellisuudessa, varsinkaan suljettujen, organisaation omien tietojärjestelmien osalta, mahdollisuuksia varmistua siitä, että rekisterinpitäjä on varmasti huolehtinut sisäänrakennetun tietosuojan vaatimuksien toteuttamisesta ja että oletusarvoinen tietosuoja varmasti toteutuu, vaan hän on pakotettu luottamaan siihen, että rekisterinpitäjä toteuttaa tietosuoja-asetusta henkilötietojen käsittelyssä.

Helsingin yliopiston kirjaston kokoelmista löytyvät pro gradu -tutkielmat aiheesta on tehty lähes täysin oikeustieteelliselle tiedekunnalle. Kolmea näistä on käsitelty ohessa niiden aiheiden ollessa varsin relevantteja tähän tutkielmaan nähden:

Sonja Vainion pro gradu -tutkielma Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa (2018) [31] tutkii osoitusvelvollisuudelle asetettuja vaatimuksia tietosuoja-asetuksessa. Tutkielmassa on todettu, että osoitusvelvollisuus korostaa rekisterinpitäjän vastuuta siitä, että henkilötietojen käsittely on tietosuoja-asetuksen mukaista, riippumatta siitä, millaiset mahdollisuudet rekisteröidyllä on vaikuttaa tietojensa käsittelyyn. Velvollisuuden täyttämisen todetaan edellyttävän dokumentaation tuottamista riippumatta siitä, onko sillä vastaanottajaa. Osoitusvelvollisuuden aktiivinen täyttäminen toimii myös itsereflektiona organisaation sisällä: sen avulla on mahdollista tarkastella, onko organisaatio toteuttanut riittävät toimenpiteet tietosuojan varmistamiseksi. Vainio toteaa kuitenkin, että rekisterinpitäjien puutteellinen tietämys tietosuoja-asetuksen vaatimuksista tietojenkäsittelylle on ollut esteenä riittävän tietosuojan toteuttamiselle. Sisäänrakennetun tietosuojan vaatimusten toteuttamisella onkin selkeä yhteys osoitusvelvollisuuden täyttymiseen. Tietosuoja-asetuksessa nimenomaisesti edellytetyt toimenpiteet ovat seloste käsittelytoimista, vaikutustenarviointi sekä tietosuojavastaavan nimittäminen. Lisäksi rekisterinpitäjällä on vapaus päättää muista osoituskeinoista kuten dokumentoinnista ja käsittelytoimien toteutumisen valvonnasta. Oman tutkielmani arviot osoitusvelvollisuuden toteuttamisen vaatimuksista vastaavat Vainion tutkielman päätelmiä.

Aaro Kuusikoski on pro gradu -tutkielmassaan Rekisterinpitäjän informointivelvollisuus – tietosuoja-asetuksen vaatimukset ja asianmukaiset toimenpiteet informaation läpinäkyvälle toimittamiselle (2019) [16] käynyt läpi informointivelvoitteen vaatimuksia ja vaaditun informaation toimittamista vastaanottajalle. Hän toteaa, että suosituin tapa esittää vaaditut tiedot on koota ne tietosuojaselosteeseen. Jos henkilötietojen luovuttaminen tapahtuu verkkosivustolla, on tutkielmassa ehdotettu informaation tarjoamista monitasoisen sähköisen tietosuojaselosteen avulla. Monitasoisuus tarkoittaa sitä, ettei kaikkia tietosuojaselosteen tietoja esitetä yhdellä sivulla peräjälkeen, vaan tiedot on jaettu osioi-

hin, joihin lukija voi perehtyä avaamalla kunkin osion erikseen. Ensimmäisellä tasolla tarjotaan lyhyemmin selostettua yleisemmän tason informaatiota käsittelytarkoituksista, rekisterinpitäjästä ja rekisteröidyn oikeuksista, ja lukija voi porautua tarkemmalle informaatiotasolle halutessaan. Kuusikosken mukaan EU:n tietosuojaneuvosto suosittelee monitasoisen tietosuojaselosteen käyttämistä digitaalisissa ympäristöissä. Tutkielmassa esitetään myös muita tapoja informointivelvoitteen täyttämiseen. Ajatus monitasoisesta tietosuojaselosteesta oli uusi, ja sen hyödyntäminen Maanmittauslaitoksen tietosuojaohjeistuksen kehittämisessä on hyvinkin käyttökelpoinen. Tutkielman ehdotuksiin voi olla hyvä palata, kun Maanmittauslaitoksessa ryhdytään määrittelemään yhteisiä käytäntöjä muun muassa informointivelvoitteen täyttämiseen.

Jesse Heiskanen on tehnyt pro gradu -tutkielman otsikolla Henkilötiedon käsite ja anonyymit tiedot eurooppalaisessa tietosuojalainsäädännössä (2019) [11]. Tutkielmassa on henkilötiedon käsitteen tutkailun jälkeen lyhyesti paneuduttu pseudonymisointiin. Siinä todetaan hyvin, että ”pseudonymisointi on ensisijaisesti nähtävissä prosessina, jossa peitetään identiteettejä”. Pseudonymisoinnin toteutustekniikaksi on suositeltu kaksisuuntaista salausalgoritmia. Oman tutkimukseni näkökulmasta, kun henkilötietoja käsitellään vain organisaation tietoverkon sisällä, on rekisteröidyn avaintaminen hänelle annetun erillisen tunnisteen avulla kuitenkin riittävä varotoimi, jos varsinaisten henkilötietojen säilytys muilta osin minimoidaan. Tietojen anonymisoinnista tutkielmassa todetaan, että tärkeä anonymisoinnin kriteeri on sen peruuttamattomuus: kun tieto on anonymisoitu, ei siitä ole enää millään konstein selvitettävissä, kehen rekisteröityyn se on liittynyt. Anonymisoinnin avulla tiedot voidaan irrottaa alkuperäisestä käyttötarkoitussidonnaisuudestaan ja mahdollistaa niiden käsittely ja analysointi muussa tarkoituksessa. Heiskanen toteaa, että anonymisointi on tekninen toimenpide, jossa tulee kuitenkin kuulla myös oikeustieteilijöitä, jotta tarvittavat näkökulmat tulevat puolin ja toisin katettua ja arvioitua. EU:n jo lakkautetun tietosuojatyöryhmän anonymisointitekniikoita koskeva lausunto 05/2014 (WP 216) [21] ohjaa tällä hetkellä parhaiten anonymisoinnin tulkintaa EU:ssa. Näistä tekniikoista tietosuojan kannalta luotettavin on karkeistaminen eli aggregointi. Tutkielman mukaan anonymisointi tulisi nähdä prosessina, jota arvioidaan ja jonka tietoturvallisuutta kehitetään. Heiskasen tutkielmassa sekä henkilötiedon käsitettä että anonymisointia on käsitelty huomattavasti yksityiskohtaisemmin kuin omassa tutkielmassani, mikä on luonnollista. Heiskasen havainnot vahvistivat omaa käsitystäni siitä, minkälaisia toimenpiteitä Maanmittauslaitoksessa tulee toteuttaa anonymisoinnin osalta.

Tietosuojaan liittyvien tutkielmien määrästä on nähtävissä, että aiheena tietosuoja-asetus

on ajankohtainen ja monipuolinen lähde varsinkin oikeustieteelliseen tutkimustyöhön. Mielenkiintoinen se on myös siksi, että usein tutkielmissa on väistämättä poikkitieteellisiä piirteitä: tietojenkäsittelytieteilijät ovat joutuneet tutustumaan lakiteksteihin, ja hyvin usein myös oikeustieteilijät ovat tutkineet tietojenkäsittelytieteen piirissä olevaa käsitteistöä. Näiden kahden tieteenalan tuntemus avaa tutkijalle monia mahdollisia tutkimuskohteita tietosuojaan liittyen.

7 Johtopäätökset

Tutkielmassa tarkasteltiin Privacy by Design -periaatteen eli sisäänrakennetun tietosuojan soveltamista henkilötietojen käsittelyssä käytettävien tietojärjestelmien sovelluskehitykseen EU:n yleisen tietosuoja-asetuksen asettamat vaatimukset huomioiden. Tutkielman aikana toteutettiin Maanmittauslaitokselle tietosuojaohjeistuksen runko sen sovelluskehitystyön tueksi.

Tietosuoja-asetuksen sovellettavaksi tuleminen vuoden 2018 toukokuussa alkaen asetti suomalaiset organisaatiot tilanteeseen, jossa niiden tuli saattaa henkilötietojen käsittelytehtävät tietosuoja-asetuksen mukaisiksi. Asetuksen suurin ero verrattuna aiempaan henkilötietolakiin oli sen rekisterinpitäjälle asettama osoitusvelvollisuus, joka terävöitti organisaatioiden suhtautumista henkilötietojen käsittelyyn selvästi. Myös Maanmittauslaitoksessa käynnistettiin kaksi projektia asetuksen velvollisuuksien huomioimiseksi. Projekteissa uusittiin henkilötietojen käsittelyyn liittyviä prosesseja ja käytäntöjä, ohjeistettiin ja koulutettiin henkilökuntaa tuntemaan organisaation tietosuojavelvollisuuksia ja selvitettiin silloisten tietovarantojen ja tietojärjestelmien tietosuoja-asetuksen mukaisuutta. Asetuksen velvoitteiden tietojärjestelmiin implementoinnin ohjeistaminen jäi kuitenkin tekemättä.

Tutkielmassa selvitettiin, minkälaisia vaatimuksia tietosuoja-asetus sekä muut henkilötietojen käsittelyä säätelevät lait aiheuttavat tietojenkäsittelylle ja sovelluskehitykselle. Lopputoteama oli, että sovelluskehitykseen vaikuttavia sisäänrakennetun tietosuojan vaatimuksia on hyvin runsaasti lähtien siitä, minkälaisella oikeudella organisaatiot henkilörekistereitä saavat pitää ja miten niiden on pystyttävä palvelemaan rekisteröityjä henkilöitä henkilötietojensa hallinnassa, ja päätyen siihen, miten rekisterinpitäjät saavat luovuttaa henkilötietoja kolmansille osapuolille ja miten niiden pitää huolehtia tietojen poistamisesta, kun ei ole enää olemassa mitään laillista syytä niiden säilyttämiselle. Sisäänrakennetun tietosuojan tulee kattaa koko henkilötiedon elinkaari. Selvää oli, että sovelluskehittäjillä ei voi olla riittävästi tietoa ja osaamista hallita kaikkia vaatimuksia ilman, että vaatimukset on heitä varten lakiteksteistä kerätty sekä kuvattu, mikä on rekisterinpitäjän tahtotila niiden toteuttamiseksi. Tietosuoja-asetuksen riskilähtöinen ajattelutapa ei vaadi kaikkien mahdollisten vaatimusten täyttämistä joka organisaatiossa ja joka käsittelytehtävässä, vaan kunkin vaatimuksen kohdalla tulee punnita sen riskit ja

kustannukset niiden ehkäisemiseksi, ja sen pohjalta toimia organisaation parhaaksi katsomalla tavalla. Näin ollen ei edes voida antaa geneerisiä ohjeita sille, miten tietosuojaa tulisi tietojärjestelmiin toteuttaa. Tässä tutkielmassa kerätyissä sisäänrakennetun tietosuojan vaatimuksissa ja niiden ripustamisessa arkkitehtuurikerroksiin ja arkkitehtuurikehittämisen vaiheisiin TOGAF-kokonaisarkkitehtuurikehyksen avulla on kuitenkin olemassa pohja, josta lähteä rakentamaan organisaation omaa mallia toteuttaa tietosuojaa tietojärjestelmiin.

Tutkielman toinen tavoite oli määrittää, minkälaista ohjeistusta sovelluskehittäjät tarvitsevat, jotta osaavat implementoida tietosuojavaatimukset tietojärjestelmiin. Tässä tutkimuskohteena olivat Maanmittauslaitoksen sovelluskehityksen asiantuntijat, joista 19:ää haastateltiin tutkimuksen aikana. Asiantuntijat saivat ideoida tapoja toteuttaa tietosuojaohjeistus sekä kertoa, millaista sisältöä ohjeissa tulisi olla. Parhaita, konkreettisia ideoita olivat toiveet tietosuojan vaatimuspankin ja vastaavasti tietosuojan testitapausjoukon toteuttamisesta: näiden avulla voitaisiin varmistua siitä, että tarvittavat tietosuojavaatimukset eivät pääse unohtumaan määrittelyistä ja että vaadittujen tietosuojaominaisuuksien testaamisestakin tulee huolehdittua. Lisäksi tarve tuottaa vaatimusmäärittelyä tekeville substanssiasiantuntijoille, kokonaisarkkitehtuuria kuvaaville arkkitehdeille ja sovelluksen lopullisen suunnittelun ja toteutuksen tekeville sovelluskehittäjille kullekin omanlaisensa vaiheistetut ohjeet oli varsin odotettu. Sisäänrakennetun tietosuojan vaatimusten kerääminen ja niiden kiinnittäminen TOGAF-vaiheisiin oli näille toiveille hyvä lähtökohta. Maanmittauslaitokselle voitiinkin niiden avulla toteuttaa jo tutkielman aikana sovelluskehitykseen tarkoitettu tietosuojaohjeistusrunko, jossa tietosuojaperiaatteet, tietosuojavaatimukset ja arkkitehtuurikehittämisen vaiheet on sidottu yhteenkuuluvaksi ohjekokonaisuudeksi. Testitapausjoukonkin toteuttaminen on suunnitelmissa. Maanmittauslaitoksella on tämän tutkielman lopputuloksena olemassa aiempaa huomattavasti vahvempi pohja, jolta lähteä suunnittelemaan henkilötietojen käsittelyä tietojärjestelmissä.

Kirjallisuus

[1] A. Cavoukian. ”Privacy by design”. *Take the challenge. Information and privacy commissioner of Ontario, Canada* (2009).

[2] *COUNCIL DECISION (EU) 2016/920 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences*. English. 2016. URL: https://ec.europa.eu/info/sites/info/files/celex_32016d0920_en_txt.pdf.

[3] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. L. Métayer, R. Tirtea ja S. Schiffner. ”Privacy and Data Protection by Design – from policy to engineering”. *CoRR* abs/1501.03726 (2015). arXiv: 1501.03726. URL: http://arxiv.org/abs/1501.03726.

[4] *Digi- ja väestötietoviraston verkkosivut, Turvakiellon hakeminen tai peruuttaminen*. URL: https://dvv.fi/turvakielto.

[5] K. Eriksson Päivi ja Koistinen. *Monenlainen tapaustutkimus*. Finnish. ID: 76855686. Helsinki: Kuluttajatutkimuskeskus, 2005. ISBN: 9516981232 9789516981232.

[6] S. Esayas. ”The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the ‘all or nothing’ approach”. *European Journal of Law and Technology* 6.2 (2015). ISSN: 2042-115X. URL: http://ejlt.org/article/view/378.

[7] *Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. EU:n yleinen tietosuoja-asetus*. Finnish. 2016. URL: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI#d1e6530-1-1.

[8] *Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta*. Finnish. 1995. URL: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:31995L0046&from=FI.

[9] *Euroopan unionin perusoikeuskirja 2016/C 202/02*. Finnish. 2016. URL: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:12016P/TXT&from=FI.

[10] *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*. English. 2019. URL: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf.

[11] J. Heiskanen. "Henkilötiedon käsite ja anonyymit tiedot eurooppalaisessa tietosuojalainsäädännössä". fin. Pro gradu -tutkielma, Helsingin yliopisto, Oikeustieteellinen tiedekunta., 2019. URL: https://helka.finna.fi/Record/helda_gradu.10138_305468.

[12] *Henkilötietolaki 523/1999*. Finnish. 1999. URL: https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523.

[13] K. Hjerppe. "Yleinen tietosuoja-asetus ja ohjelmistoarkkitehtuuri". fin. Pro gradu -tutkielma, Turun yliopisto, Luonnontieteiden ja tekniikan tiedekunta., 2018. URL: https://finna.fi/Record/utupub_masters.10024_145453.

[14] *JHS 179 Kokonaisarkkitehtuurin suunnittelu ja kehittäminen*. Finnish. 2011. URL: http://www.jhs-suositukset.fi/web/guest/jhs/recommendations/179/full.

[15] P. Korpisaari. *Henkilötiedot ja paikkatiedot. Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen*. Finnish. 2018. URL: http://urn.fi/URN:ISBN:978-952-11-4787-6.

[16] A. Kuusikoski. "Rekisterinpitäjän informointivelvollisuus – tietosuoja-asetuksen vaatimukset ja asianmukaiset toimenpiteet informaation läpinäkyvälle toimittamiselle". Pro gradu -tutkielma, Helsingin yliopisto, Oikeustieteellinen tiedekunta., 2019. URL: https://helka.finna.fi/Record/helda_gradu.10138_310999.

[17] *Laki julkisen hallinnon tiedonhallinnasta 906/2019*. Finnish. 2019. URL: https://www.finlex.fi/fi/laki/alkup/2019/20190906#Pidp446153600.

[18] *Laki kiinteistötietojärjestelmästä ja siitä tuotettavasta tietopalvelusta 453/2002*. Finnish. 2002. URL: https://www.finlex.fi/fi/laki/ajantasa/2002/20020453.

[19] *Laki viranomaisten toiminnan julkisuudesta 621/1999*. Finnish. 1999. URL: https://www.finlex.fi/fi/laki/ajantasa/1999/19990621.

[20] *Laki yksityisyyden suojasta työelämässä 759/2004*. Finnish. 2004. URL: https://www.finlex.fi/fi/laki/ajantasa/2004/20040759#L2P5.

[21] *Lausunto 5/2014 anonymisointitekniikoista*. Finnish. 2014. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fi.pdf.

[22] *Maanmittauslaitoksen sisäiset ohjeet ja tietosuojaprojektimateriaalit*. 2017–2019.

[23] *Maanmittauslaitoksen verkkosivut*. URL: https://www.maanmittauslaitos.fi/.

[24] *Open Group Standard, TOGAF Version 9.1*. The Open Group, 2011. ISBN: ISBN: 9789087536794. URL: https://pubs.opengroup.org/architecture/togaf91-doc/arch/.

[25] K. Peffers, T. Tuunanen, M. A. Rothenberger ja S. Chatterjee. "A Design Science Research Methodology for Information Systems Research". *Journal of Management Information Systems* 24.3 (2007), s. 45–77. DOI: 10.2753/MIS0742-1222240302.

[26] J. van Rest, D. Boonstra, M. Everts, M. van Rijn ja R. van Paassen. "Designing Privacy-by-Design". Teoksessa: *Privacy Technologies and Policy*. Toim. B. Preneel ja D. Ikonomou. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, s. 55–72. ISBN: 978-3-642-54069-1.

[27] *Suomen perustuslaki 731/1999*. Finnish. 1999. URL: https://www.finlex.fi/fi/laki/ajantasa/1999/19990731.

[28] *Suositus tiedonhallintamallista*. Finnish. URL: http://urn.fi/URN:ISBN:978-952-367-328-1.

[29] *Tietosuojalaki 1050/2018*. Finnish. 2018. URL: https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.

[30] *VAHTI-raportti 1/2016. EU-tietosuojan kokonaisuudistus*. Finnish. 2016. URL: https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229.

[31] S. Vainio. "Rekisterinpitäjän osoitusvelvollisuus EU:n yleisessä tietosuoja-asetuksessa". fin. Pro gradu -tutkielma, Helsingin yliopisto, Oikeustieteellinen tiedekunta., 2018. URL: https://helka.finna.fi/Record/helda_gradu.10138_232856.

[32] M. Westerlund. "A study of EU data protection regulation and appropriate security for digital services and platforms". eng. Tohtorinväitöskirja. Information systems, Faculty of Social Science, Business ja Economics.; Åbo Akademi, fakulteten för samhällsvetenskaper och ekonomi, informationssystem, 2018, xiv, 168 sivua, 103 sivua useina numerointijaksoina. ISBN: 978-952-12-3693-8 nidottu. URL: https://finna.fi/Record/jykdok.2002243.

Liite A Tietosuojavaatimukset

Taulukossa on esitetty kaikki ne sisäänrakennettuun tietosuojaan liittyvät vaatimukset, jotka on kerätty ja luokiteltu tutkielman kappaleessa 3. Taulukkoon on merkitty, missä TOGAF-kokonaisarkkitehtuuriviitekehyksen ADM-arkkitehtuurikehittämisprosessin vaiheissa ne tulee käsitellä [24]. ADM:n vaihe C. Tietojärjestelmäarkkitehtuuri (Information Systems Architecture) on jaettu taulukossa kahteen osaan. Taulukkoesityksessä käytetyt ADM-prosessin vaiheet ovat:

A. Arkkitehtuurivisio (Architecture Vision)

B. Toiminta-arkkitehtuuri (Business Architecture)

C1. Tietoarkkitehtuuri (Information Systems Architecture, data architecture)

C2. Sovellusarkkitehtuuri (Information Systems Architecture, application architecture)

D. Teknologia-arkkitehtuuri (Technology Architecture)

E. Mahdollisuudet ja ratkaisut (Opportunities and Solutions)

F. Siirtymäsuunnittelu (Migration Planning)

G. Toteutuksen hallinta (Implementation Governance)

H. Arkkitehtuurin hallinta (Architecture Change Management)

Lisäksi omana vaiheenaan on merkitty ADM-malliin kuulumaton sovelluskehitysvaihe, joka saa syötteensä F-vaiheelta ja jota G-vaihe ohjaa.

Kukin vaatimus voi vaatia käsittelyä useammassa vaiheessa. Sovelluskehitykseen suoraan vaikuttavat sisäänrakennetun tietosuojan arkkitehtuurivaatimukset käsitellään vaiheissa B, C ja D, joiden lopputuotoksena syntyvää arkkitehtuuridokumentaatiota vielä täsmennetään ja tarkennetaan vaiheissa E ja F. Kahta vaatimuksista käsitellään vasta sovelluskehitysvaiheessa. Vaiheissa A, G ja H huomioitavat vaatimukset ovat pääosin kehittämistyön perusteisiin ja organisatoristen toimenpiteiden toteuttamiseen liittyviä vaatimuksia.

Tunnus	Teksti	A	B	C1	C2	D	E	F	sovkeh	G	H
1.0	Rekisterinpitäjän on tunnistettava, käsitelläänkö kehitettävässä tietojärjestelmässä henkilötietoja.	x									x
1.1	Rekisterinpitäjän on tunnistettava rekisteröitävät suorat ja epäsuorat			x							
1.2	Rekisterinpitäjän on varmistettava oikeus tallentaa rekisteröidyn henkilötunnus, jos se tunnistetaan rekisteröitäväksi henkilötiedoksi.			x							
1.3	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta käsitellä käyttöliittymässä ilman erityistä tarvetta.				x				x		
1.4	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta merkitä tulosteisiin ilman erityistä tarvetta.				x				x		
1.5	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta luovuteta ilman lakisääteistä oikeutta sen luovuttamiseen.				x				x		
1.6	Rekisterinpitäjän (viranomainen) on pyrittävä hyödyntämään jo kerättyjä henkilötietoja, jos niitä on saatavissa toiselta viranomaiselta.		x	x	x	x	x		x		
2.1	Rekisterinpitäjän on tunnistettava lainmukainen peruste henkilötietojen	x									
2.2	Rekisteröidyn on saatava riittävät tiedot henkilötietojen käsittelystä henkilötietojen rekisteröintiin suostumuksen tueksi.				x				x		
2.3	Rekisteröidyn on voitava antaa suostumuksensa henkilötietojen rekisteröintiin yksinkertaisella, selkeällä, yksikäsitteisellä tavalla.		x		x		x		x		
2.4	Rekisterinpitäjän on voitava osoittaa rekisteröidyn tekemä suostumus annetuksi.			x					x		
2.5	Rekisterinpitäjän on voitava osoittaa, mihin henkilötietojen käyttötarkoitukseen liittyen rekisteröity on antanut suostumuksensa.			x					x		
2.6	Rekisteröidyn on voitava peruuttaa suostumuksensa yhtä helposti kuin on sen				x		x		x		
3.1	Rekisterinpitäjän on tunnistettava mahdolliset arkaluonteiset rekisteröitävät			x							
3.2	Rekisterinpitäjän on rajoitettava arkaluonteisten henkilötietojen käsittelyä riittävin tietoteknisin ratkaisuin.				x				x		
3.3	Rekisterinpitäjän on suostumuksen antamisen yhteydessä mahdollisuuksien mukaan varmistuttava siitä, että rekisteröitävä on vähintään 13-vuotias.		x		x		x		x		
3.3.1	Rekisterinpitäjän on ilmaistava palvelun ikäraja selkeästi suostumuksen antamisen yhteydessä, jos palvelu ei vaadi vahvaa tunnistautumista.				x		x				
3.3.2	Rekisteröitävän huoltajalle on tarjottava ratkaisu suostumuksen tai valtuutuksen antamiseen, jos rekisteröitävä on alle 13-vuotias.			x	x						
3.3.3	Lapsen voitava rekisteröityä palveluun ilman huoltajan hyväksymistä, jos kyseessä on lapsille suunnattu ennalta ehkäisevä tai neuvontapalvelu.				x						
4.1	Rekisteröidyn on saatava määrätyt tiedot henkilötietojensa käsittelystä helposti ymmärrettävässä, selkeässä muodossa.		x		x		x		x		x
4.2	Rekisteröidyn on saatava henkilötiedot antaessaan riittävä tieto rekisteröidyn oikeuksista ja siitä, miten hänen on mahdollista käyttää oikeuksiaan, sekä		x		x		x		x		x
4.3	Rekisteröidyn on voitava antaa tarvittavat tiedot rekisteröintiä varten.			x	x		x		x		
4.4	Rekisterinpitäjän on voitava tunnistaa, mistä rekisteröidyn henkilötiedot on			x	x				x		
4.5	Rekisteröidylle on ilmoitettava kuukauden sisällä, jos hänen henkilötietojaan saadaan muualta kuin rekisteröidyltä itseltään.		x		x				x		
4.6	Rekisterinpitäjän on tiedettävä, koska rekisteröity on saanut tiedon henkilötietojensa saamisesta.			x					x		
4.7	Rekisteröidyn on saatava tieto siitä, jos kerättyjen henkilötietojen käsittelytarkoitusta laajennetaan.	x	x								x
4.8	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä luettavassa, sähköisessä				x				x		
4.9	Rekisteröidyn on voitava ilmoittaa virheellisistä tiedoista tai korjata ne itse.		x		x				x		
4.10	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava korjata virheelliset				x				x		
4.11	Rekisterinpitäjän on määriteltävä, milloin tietojen poistaminen on mahdollista.	x									
4.12	Rekisteröidyn on voitava pyytää tietojen poistamista tai poistaa ne itse.		x		x				x		
4.13	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa henkilötiedot			x	x				x		
4.14	Rekisteröidyn on voitava vaatia yksilöidysti henkilötietojen käsittelyn		x								
4.15	Rekisterinpitäjän on määriteltävä, milloin tietojen käsittelyn rajoittaminen on	x									
4.16	Rekisterinpitäjän on määriteltävä, minkä henkilötietoryhmien käsittelyä on		x								
4.17	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä rekisteröidyn tietoihin kyseisten tietojen käsittelyrajoitus.			x	x				x		
4.18	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava ohittaa käsittelyrajoitetut henkilötiedot.				x				x		
4.19	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan tietojärjestelmästä tieto siitä, kenelle rekisteröidyn tiedot on luovutettu.			x	x				x		
4.20	Rekisterinpitäjän on voitava toimittaa tietojen oikaisu-, poisto- tai rajoituspyyntö kaikille niille tahoille, joille se on luovuttanut kyseisen rekisteröidyn tiedot.		x								
4.21	Rekisteröidyn on voitava ilmoittaa halustaan siirtää henkilötiedot toiseen		x								
4.22	Rekisterinpitäjän on määriteltävä, milloin tietojen siirtäminen tietojärjestelmästä toiseen on mahdollista.	x									
4.23	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä sähköisessä, koneellisesti				x				x		
4.24	Rekisterinpitäjän on määriteltävä, milloin henkilötietojen käsittelyn vastustaminen tai automaattisen päätöksenteon tai profiloinnin kieltäminen on	x									
4.25	Rekisteröidyn on voitava vastustaa henkilötietojen käsittelyä tai kieltäytyä automaattisesta päätöksenteosta ja/tai profiloinnista.		x								
4.26	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä automaattisen päätöksenteon ja profiloinnin kielto rekisteröidyn tietoihin.			x	x				x		
4.27	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava käsitellä manuaalisesti automaattisesta päätöksenteosta estetyt henkilötiedot.				x				x		
4.28	Rekisterinpitäjän on määritettävä, miten rekisteröity tunnistetaan niillä tiedoilla, jotka hänestä on olemassa.		x								
4.29	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava tunnistaa rekisteröity, joka haluaa käyttää rekisteröidyn oikeuksiaan.		x	x	x				x		

Tunnus	Teksti	A	B	C1	C2	D	E	F	sovkeh	G	H
5.1	Rekisterinpitäjän on huomioitava määritetyt käsittelyperiaatteet henkilötietojen		x	x	x	x	x				
5.2	Rekisterinpitäjän on määritettävä kerättävien tietojen käsittelytarkoitus.	x									
5.3	Rekisterinpitäjän on määritettävä rekisteröitävät tiedot mahdollisimman niukoiksi ja vain määritettyä käsittelytarkoitusta silmällä pitäen.			x							
5.4	Rekisterinpitäjän on mahdollisuuksien mukaan huolehdittava rekisteröidyn tietojen ajantasaisuudesta tietoteknisin keinoin.				x	x	x		x		
5.5	Rekisterinpitäjän on määriteltävä henkilötietojen säilytysaika mahdollisimman		x								
5.6	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa tai anonymisoida henkilötiedot säilytysajan päätyttyä.				x				x		
5.7	Rekisterinpitäjän on suojattava henkilötiedot mahdollisimman hyvin asiattomalta				x	x	x				
5.7.1	Rekisterinpitäjän on suojattava henkilötietojen käsittely soveltuvin				x				x		
5.7.2	Rekisterinpitäjän on suojattava henkilötietojen käsittely-ympäristö soveltuvin teknisin ratkaisuin ja käyttövaltuuksin.					x			x		
5.8	Rekisterinpitäjän on varmistettava, että määritelty säilytysaika huomioi		x								
5.9	Rekisterinpitäjän on tiedettävä, minne kaikkialle henkilötieto on tallennettu ja			x	x		x		x		
5.10	Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja.				x	x			x		
5.11	Rekisterinpitäjän on huolehdittava henkilötietojen minimoinnista, jos henkilötietoja säilytetään erityisiä käsittelytarkoituksia varten.			x	x				x		
6.1	Rekisterinpitäjän on varmistuttava henkilötietojen siirron tai luovutuksen		x								
6.2	Rekisterinpitäjän on huolehdittava henkilötietojen näkyvyyden rajoittamisesta				x				x		
6.3	Rekisteröidyn on voitava antaa suostumus tietojen luovuttamiseen, jos tietoja luovutetaan suoramarkkinointiin tai mielipide- tai markkinatutkimuksiin		x	x	x				x		
6.4	Rekisteröidyn on voitava perua suostumuksensa tietojen luovuttamiseen				x				x		
6.5	Rekisterinpitäjän (viranomainen) on toteutettava tietovarantonsa niin, että myös muut viranomaiset voivat niitä hyödyntää.			x	x	x	x		x		
6.6	Rekisterinpitäjän (viranomainen) on voitava tunnistaa luovutettujen tietojen				x	x	x		x		
6.7	Rekisterinpitäjän (viranomainen) on kerättävä lokia tiedonluovutuksista.				x	x	x		x		
6.8	Rekisterinpitäjän (viranomainen) on varmistuttava tiedonluovutuksen		x								
6.9	Rekisterinpitäjän (viranomainen) on huolehdittava siitä, ettei käyttöliittymässä ole näkyvissä tarpeettomia tietoja.				x				x		
6.10	Rekisterinpitäjän (viranomainen) on rekisteröitävä tietopyynnöt asiarekisteriin.		x						x		
6.11	Rekisterinpitäjän on varmistuttava henkilötietojen luovuttamisen kolmansiin maihin lainmukaisuudesta.		x								
6.12	Rekisterinpitäjän on kirjattava arviointi tiedonsiirrosta ja toteutetut suojatoimet tietosuojaselosteeseen.										
7.1	Henkilötietojen käsittelijällä tulee olla oikeudet vain hänen tehtäviensä kannalta tarpeellisiin tietoihin.		x		x				x		
7.2	Rekisterinpitäjän on huolehdittava, ettei henkilötietojen käsittelijä pääse käsittelemään tarpeettomia henkilötietoja.		x		x				x		
7.3	Rekisterinpitäjän on huolehdittava henkilötietoja käsittelevän tietojärjestelmän riskiarvioinnista ja sen perusteella tehtävistä toimenpiteistä.	x	x				x			x	
7.4	Rekisterinpitäjän on huolehdittava vaikutustenarvioinnista, mikäli henkilötietojen käsittelyssä havaitaan mahdollisuus korkeaan riskitasoon.	x									
7.5	Rekisterinpitäjän (viranomainen) on toteutettava henkilörekisterinsä vikasietoisiksi ja palautumiskykyisiksi.					x	x				
7.6	Rekisterinpitäjän (viranomainen) on toteutettava sähköiset tiedonsiirrot salattuja tai suojattuja yhteyksiä käyttäen.					x	x				
7.7	Rekisterinpitäjän (viranomainen) on huolehdittava, ettei henkilörekistereihin ole oikeuksia kuin heillä, joilla tietojen käsittely kuuluu työtehtäviin.		x		x				x	x	
7.8	Rekisterinpitäjän (viranomainen) on kerättävä lokia tietojärjestelmän käytöstä.				x		x		x		
8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin.					x	x		x		
8.2	Rekisterinpitäjän on testattava henkilötietoja käsittelevät järjestelmät sen varmistamiseksi, ettei tietoja vuoda vääriin käsiin.								x		
8.3	Rekisterinpitäjän on huolehdittava henkilötietojen käsittelyn lokittamisesta, jotta pystytään selvittämään loukatut rekisteröidyt ja henkilötiedot.				x	x	x		x		
8.4	Rekisterinpitäjän on salattava sen tietovälineille tallennettu data.					x	x		x		
8.5	Rekisterinpitäjän on tarkistettava henkilötietoja sisältävien palveluiden käyttöoikeudet säännöllisesti.										x
8.6	Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla tietoturvaloukkaukset olisi				x				x		
8.7	Rekisterinpitäjän (viranomainen) on pyrittävä määrittelemään ja löytämään tietovarantoihinsa tehtävät poikkeavat haut.								x		
9.1	Rekisterinpitäjän on liitettävä tietosuojaseloste rekisteröidyille tarjottaviin palveluihin näiden nähtäväksi.				x				x		x
9.2	Rekisterinpitäjän on huolehdittava tietosuojaselosteen ajantasaisuudesta.										x
9.3	Rekisterinpitäjän (viranomainen) on dokumentoitava rekisteröidyt henkilötiedot ja niiden käsittelijät.										x
9.4	Rekisterinpitäjän (viranomainen) on kuvattava henkilötietovirrat rekistereittäin sisältäen tietolähteet, tietoja käyttävät tietojärjestelmät, henkilötietojen siirrot järjestelmien välillä ja henkilötietojen käsittelyn fyysiset sijainnit.										x
9.5	Rekisterinpitäjän (viranomainen) on dokumentoitava tiedonluovutukset ja siirrot kolmansille osapuolille sekä niiden perusteet.										x
9.6	Rekisterinpitäjän (viranomainen) on kuvattava henkilötietojen säilytysajat ja										x
9.7	Rekisterinpitäjän (viranomainen) on kuvattava tietoturvallisuustoimenpiteet, joiden avulla henkilörekisterien turvallisuus on toteutettu.										x

Liite B Tietosuojaohjeistusesimerkki

Tutkielman kappaleessa 5.3 on esimerkki siitä, miten Maanmittauslaitokselle tutkielman lopputuloksena toteutettua tietosuojaohjeistoa on mahdollista hyödyntää. Kyseiseen esimerkkiin liittyvät sivut ohjeiston kolmesta toteutetusta tietosuojasivutyypistä on kerätty tähän liitteeseen:

- Tietosuojavaatimukset-sivu
- Tietosuojaperiaatteet-sivujen esimerkkinä on Käsittelyperiaatteiden huomioiminen -sivu
- Vaihekohtaiset vaatimussivujen esimerkkinä ovat B. Toiminta-arkkitehtuuri- ja C2. Sovellusarkkitehtuuri -sivut

Sivutyyppien väliset suhteet on kuvattu tutkielman kappaleessa 5.3 kuvassa 5.1.

Tietosuojavaatimukset

Tietosuoja-asetuksesta, tietosuojalaista ja tiedonhallintalaista on kerätty sovelluskehitykseen vaikuttavia vaatimuksia, jotka pitää huomioida jokaisessa tietojärjestelmänprojektissa ja tuotannossa olevan tietojärjestelmän uuden version toteutuksessa. Vaatimukset on numeroitu, jolloin niihin voidaan viitata vaatimuksen tunnuksella myös muilta sivuilta. Kullekin vaatimukselle on merkitty, missä arkkitehtuurikehityksen vaiheessa se on käsiteltävä. Arkkitehtuurikehityksen vaiheet on nimetty TOGAF-kokonaisarkkitehtuuriviitekehyksen tunnusten mukaisesti. Taulukon otsikoissa käytetyt vaiheet ovat:

- A. Arkkitehtuurivisio (Architecture Vision)
- B. Toiminta-arkkitehtuuri (Business Architecture)
- C1. Tietoarkkitehtuuri (Information Systems Architecture, data architecture)
- C2. Sovellusarkkitehtuuri (Information Systems Architecture, application architecture)
- D. Teknologia-arkkitehtuuri (Technology Architecture)
- E. Arkkitehtuurikomponenttien valinta (Opportunities and Solutions)
- H. Arkkitehtuurin hallinta (Architecture Change Management)

TOGAFin vaiheille F. Migraatiosuunnitteu (Migration Planning) ja G. Toteutuksen hallinta (Implementation Governance) ei tunnistettu omia sovelluskehitysvaatimuksia.

Erikseen on kuvattu, miten vaatimukset tulee huomioida varsinaisen sovelluskehitysprosessin aikana.

Rekisteröitävien henkilötietojen tunnistaminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
1.0	Rekisterinpitäjän on tunnistettava, käsitelläänkö kehitettävässä tietojärjestelmässä henkilötietoja		x						x
1.1	Rekisterinpitäjän on tunnistettava rekisteröitävät suorat ja epäsuorat henkilötiedot				x				
1.2	Rekisterinpitäjän on varmistettava oikeus tallentaa rekisteröidyn henkilötunnus, jos se tunnistetaan rekisteröitäväksi henkilötiedoksi				x				
1.3	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta käsitellä käyttöliittymässä ilman erityistä tarvetta					x			
1.4	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta merkitä tulosteisiin ilman erityistä tarvetta					x			
1.5	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta luovuteta ilman lakisääteistä oikeutta sen luovuttamiseen					x			
1.6	Rekisterinpitäjän on pyrittävä hyödyntämään jo kerättyjä henkilötietoja, jos niitä on saatavissa toiselta viranomaiselta			x	x	x	x	x	

Käsittelyn oikeusperusteen tunnistaminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
2.1	Rekisterinpitäjän on tunnistettava lainmukainen peruste henkilötietojen käsittelylle		x						
2.2	Rekisteröidyn on saatava riittävät tiedot henkilötietojen käsittelystä henkilötietojen rekisteröintiin suostumuksen tueksi					x			
2.3	Rekisteröidyn on voitava antaa suostumuksensa henkilötietojen rekisteröintiin yksinkertaisella, selkeällä, yksiselitteisellä tavalla			x		x		x	
2.4	Rekisterinpitäjän on voitava osoittaa rekisteröidyn tekemä suostumus annetuksi				x				
2.5	Rekisterinpitäjän on voitava osoittaa, mihin henkilötietojen käsittelytarkoitukseen liittyen rekisteröity on antanut suostumuksensa				x				
2.6	Rekisteröidyn on voitava peruuttaa suostumuksensa yhtä helposti kuin on sen antanut					x		x	

Arkaluonteisten henkilötietojen tunnistaminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
3.1	Rekisterinpitäjän on tunnistettava mahdolliset arkaluonteiset rekisteröitävät henkilötiedot				x				
3.2	Rekisterinpitäjän on rajoitettava arkaluonteisten henkilötietojen käsittelyä riittävin tietoteknisin ratkaisuin					x			
3.2.1	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä yhteystietojen salassapitopäätös tietojärjestelmään	Lisävaatimus MML:n tarpeisiin				x			
3.3	Rekisterinpitäjän on suostumuksen antamisen yhteydessä mahdollisuuksien mukaan varmistuttava, että rekisteröitävä on vähintään 13-vuotias	Kun rekisteröinti perustuu suostumukseen		x		x		x	
3.3.1	Rekisterinpitäjän on ilmaistava palvelun ikäraja selkeästi suostumuksen antamisen yhteydessä	Kun rekisteröinti perustuu suostumukseen				x			
3.3.2	Rekisteröitävän huoltajalle on tarjottava mahdollisuus antaa suostumus tai valtuutus, jos rekisteröitävä on alle 13-vuotias	Kun rekisteröinti perustuu suostumukseen			x	x			
3.3.3	Lapsen on voitava rekisteröityä palveluun ilman huoltajan hyväksymistä, jos kyseessä on lapsille suunnattu ennalta ehkäisevä tai neuvontapalvelu	Ei koske MML:sta							

Rekisteröidyn oikeuksien huomioiminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
4.1	Rekisteröidyn on saatava määrätyt tiedot henkilötietojensa käsittelystä helposti ymmärrettävässä, selkeässä muodossa			x		x		x	x
4.2	Rekisteröidyn on saatava henkilötiedot antaessaan riittävä tieto rekisteröidyn oikeuksista ja siitä, miten hänen on mahdollista käyttää oikeuksiaan, sekä tietojen säilytysajasta			x		x		x	x
4.3	Rekisteröidyn on voitava antaa tarvittavat tiedot rekisteröintiä varten				x	x		x	
4.4	Rekisterinpitäjän on voitava tunnistaa, mistä rekisteröidyn henkilötiedot on saatu				x	x			
4.5	Rekisteröidylle on ilmoitettava kuukauden sisällä, jos hänen henkilötietojaan saadaan muualta kuin rekisteröidyltä itseltään			x		x			
4.6	Rekisterinpitäjän on tiedettävä, koska rekisteröity on saanut tiedon henkilötietojensa saamisesta				x				
4.7	Rekisteröidyn on saatava tieto siitä, jos kerättyjen henkilötietojen käsittelytarkoitusta laajennetaan		x	x					x
4.8	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä luettavassa, sähköisessä muodossa nopeasti ja luotettavasti					x			
4.9	Rekisteröidyn on voitava ilmoittaa virheellisistä tiedoista tai korjata ne itse			x		x			
4.10	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava korjata virheelliset tiedot					x			
4.11	Rekisterinpitäjän on määriteltävä, milloin tietojen poistaminen on mahdollista		x						
4.12	Rekisteröidyn on voitava pyytää tietojen poistamista tai poistaa ne itse			x		x			
4.13	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa henkilötiedot tarvittaessa				x	x			
4.14	Rekisteröidyn on voitava vaatia yksilöidysti henkilötietojen käsittelyn rajoittamista			x					
4.15	Rekisterinpitäjän on määriteltävä, milloin tietojen käsittelyn rajoittaminen on mahdollista		x						
4.16	Rekisterinpitäjän on määriteltävä, minkä henkilötietoryhmien käsittelyä on mahdollista rajoittaa			x					
4.17	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä rekisteröidyn tietoihin kyseisten tietojen käsittelyrajoitus				x	x			
4.18	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava ohittaa käsittelyrajoitetut henkilötiedot					x			
4.19	Rekisterinpitäjän tai henkliötietojen käsittelijän on pystyttävä tuottamaan tietojärjestelmästä tieto siitä, kenelle rekisteröidyn tiedot on luovutettu				x	x			
4.20	Rekisterinpitäjän on voitavat toimittaa tietojen oikaisu-, poisto- tai rajoituspyyntö kaikille niille tahoille, joille se on luovuttanut kyseisen rekisteröidyn tiedot			x					
4.21	Rekisteröidyn on voitava ilmoittaa halustaan siirtää henkilötiedot toiseen tietojärjestelmään	Ei koske MML:sta							
4.22	Rekisterinpitäjän on määriteltävä, milloin tietojen siirtäminen tietojärjestelmästä toiseen on mahdollista	Ei koske MML:sta							
4.23	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä sähköisessä, koneellisesti luettavassa muodossa	Ei koske MML:sta							
4.24	Rekisterinpitäjän on määriteltävä, milloin henkilötietojen käsittelyn vastustaminen tai automaattisen päätöksenteon tai profiloinnin kieltäminen on mahdollista		x						
4.25	Rekisteröidyn on voitaa vastustaa henkilötietojen käsittelyä tai kieltäytyä automaattisesta päätöksenteosta ja/tai profiloinnista			x					
4.26	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä automaattisen päätöksenteon ja profiloinnin kielto rekisteröidyn tietoihin				x	x			
4.27	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava käsitellä manuaalisesti automaattisesta päätöksenteosta estetyt henkilötiedot					x			
4.28	Rekisterinpitäjän on määritettävä, miten rekisteröity tunnistetaan niillä tiedoilla, jotka hänestä on olemassa			x					
4.29	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava tunnistaa rekisteröity niillä tiedoilla, jotka hänestä on olemassa			x	x	x			

Käsittelyperiaatteiden huomioiminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
5.1	Rekisterinpitäjän on huomioitava määritetyt käsittelyperiaatteet henkilötietojen käsittelyssä			x					
5.2	Rekisterinpitäjän on määritettävä kerättävien tietojen käsittelytarkoitus		x						
5.3	Rekisterinpitäjän on määritettävä rekisteröitävät tiedot mahdollisimman niukoiksi ja vain määritettyä käsittelytarkoitusta silmällä pitäen				x				
5.4	Rekisterinpitäjän on mahdollisuuksien mukaan huolehdittava rekisteröidyn tietojen ajatasaisuudesta tietoteknisin keinoin					x	x	x	
5.5	Rekisterinpitäjän on määriteltävä henkilötietojen säilytysaika mahdollisimman lyhyeksi			x					
5.6	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa tai anonymisoida henkilötiedot säilytysajan päätyttyä					x			
5.7	Rekisterinpitäjän on suojattava henkilötiedot mahdollisimman hyvin asiattomalta pääsyltä					x	x	x	
5.7.1	Rekisterinpitäjän on suojattava henkilötietojen käsittely soveltuvin käyttövaltuuksin					x			
5.7.2	Rekisterinpitäjän on suojattava henkilötietojen käsittely-ympäristö soveltuvin teknisin ratkaisuin ja käyttövaltuuksin						x		

5.8	Rekisterinpitäjän on varmistettava, että määritelty säilytysaika huomioi erillislainsäädännön			x					
5.9	Rekisterinpitäjän on tiedettävä, minne kaikkialle henkilötieto on tallennettu ja monistettu				x	x		x	
5.10	Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja					x	x		
5.11	Rekisterinpitäjän on huolehdittava henkilötietojen minimoinnista, jos henkilötietoja säilytetään erityisiä käsittelytarkoituksia varten				x	x			

Henkilötietojen siirto ja luovuttaminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
6.1	Rekisterinpitäjän on varmistuttava henkilötietojen siirron tai luovutuksen lainmukaisuudesta			x					
6.2	Rekisterinpitäjän on huolehdittaa henkilötietojen näkyvyyden rajoittamisesta soveltuvin osin					x			
6.3	Rekisteröidyn on voitava antaa suostumus tietojen luovuttamiseen, jos tietoja luovutetaan suoramarkkinointiin tai mielipide- tai markkinatutkimuksiin	Ei koske MML:sta: henkilötietoja ei koskaan luovuteta näihin tarkoituksiin							
6.4	Rekisteröidyn on voitava perua suostumuksensa tietojen luovuttamiseen	Ei koske MML:sta							
6.5	Rekisterinpitäjän on toteutettava tietovarantonsa niin, että myös muut viranomaiset voivat niitä hyödyntää				x	x	x	x	
6.6	Rekisterinpitäjän on voitava tunnistaa luovutettujen tietojen vastaanottaja					x	x	x	
6.7	Rekisterinpitäjän on kerättävä lokia tiedonluovutuksista					x	x	x	
6.8	Rekisterinpitäjän on varmistuttava tietonluovutuksen tarpeellisuudesta			x					
6.9	Rekisterinpitäjän on huolehdittava siitä, ettei käyttöliittymässä ole näkyvissä tarpeettomia tietoja					x			
6.10	Rekisterinpitäjän on rekisteröitävä tietopyynnöt asiarekisteriin			x					
6.11	Rekisterinpitäjän on varmistuttava henkilötietojen luovuttamisen kolmansiin maihin lainmukaisuudesta			x					
6.12	Rekisterinpitäjän on kirjattava arviointi tiedonsiirrosta ja toteutetut suojatoimet tietosuojaselosteeseen								x

Henkilötietojen turvallisuuden varmistaminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
7.1	Henkilötietojen käsittelijällä tulee olla oikeudet vain hänen tehtäviensä kannalta tarpeellisiin tietoihin			x		x			
7.2	Rekisterinpitäjän on huolehdittava, ettei henkilötietojen käsittelijä pääse käsittelemään tarpeettomia henkilötietoja			x		x			
7.3	Rekisterinpitäjän on huolehdittava henkilötietoja käsittelevän tietojärjestelmän riskiarvioinnista ja sen perusteella tehtävistä toimenpiteistä		x	x				x	
7.4	Rekisterinpitäjän on huolehdittava vaikutustenarvioinnista, mikäli henkilötietojen käsittelyssä havaitaan mahdollisuus korkeaan riskitasoon		x						
7.5	Rekisterinpitäjän on toteutettava henkilörekisterinsä vikasietoisiksi ja palautumiskykyisiksi						x	x	
7.6	Rekisterinpitäjän on toteutettava sähköiset tiedonsiirrot salattuja ja/tai suojattuja yhteyksiä käyttäen						x	x	
7.7	Rekisterinpitäjän on huolehdittava, ettei henkilörekisterihin ole oikeuksia kuin heillä, joilla tietojen käsittely kuuluu työtehtäviin			x		x			
7.8	Rekisterinpitäjän on kerättävä lokia tietojärjestelmän käytöstä					x		x	

Henkilötietojen tietoturvaloukkausten havaitseminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin						x	x	
8.2	Rekisterinpitäjän on testattava henkilötietoja käsittelevät järjestelmät sen varmistamiseksi, ettei tietoja vuoda vääriin käsiin	Tehdään sovelluskehitysvaiheen aikana							
8.3	Rekisterinpitäjän on huolehdittava henkilötietojen käsittelyn lokittamisesta, jotta pystytään selvittämään loukatut rekisteröidyt ja henkilötiedot					x	x	x	
8.4	Rekisterinpitäjän on salattava tietovälineille tallennettu data						x	x	
8.5	Rekisterinpitäjän on tarkistettava henkilötietoja sisältävien palveluiden käyttöoikeudet säännöllisesti								x
8.6	Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla tietoturvaloukkaukset olisi mahdollista havaita					x			
8.7	Rekisterinpitäjän on pyrittävä määrittelemään ja löytämään tietovarantoihinsa tehtävät poikkeavat haut	Tehdään sovelluskehitysvaiheen aikana							

Osoitusvelvollisuuden täyttäminen

#	Otsikko	Huomautukset	A	B	C1	C2	D	E	H
9.1	Rekisterinpitäjän on liitettävä tietosuojaseloste rekiseröidyille tarjottaviin palveluihin näiden nähtäväksi					x			x
9.2	Rekisterinpitäjän on huolehdittava tietosuojaselosteen ajantasaisuudesta								x
9.3	Rekisterinpitäjän on dokumentoitava rekisteröidyt henkilötiedot ja niiden käsittelijät								x
9.4	Rekisterinpitäjän on kuvattava henkilötietovirrat rekistereittäin sisältäen tietolähteet, tietoja käyttävät tietojärjestelmät, henkilötietojen siirrot järjestelmien välillä ja henkilötietojen käsittelyn fyysiset sijainnit								x
9.5	Rekisterinpitäjän on dokumentoitava tiedonluovutukset ja siirrot kolmansille osapuolille sekä niiden perusteet								x
9.6	Rekisterinpitäjän on kuvattava henkilötietojen säilytysajat ja poistomekanismit								x
9.7	Rekisterinpitäjän on kuvattava tietoturvallisuustoimenpiteet, joiden avulla henkilörekisterin turvallisuus on toteutettu								x

Käsittelyperiaatteiden huomioiminen

Rekisterinpitäjän velvollisuutena on noudattaa tietosuoja-asetuksessa määritettyjä käsittelyperiaatteita.

Henkilötietojen käsittelyperiaatteet:

- Lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate
- Käyttötarkoitussidonnaisuuden periaate
- Tietojen minimoinnin periaate
- Täsmällisyyden periaate
- Säilytyksen rajoittamisen periaate
- Eheyden ja luottamuksellisuuden periaate

Lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate:

> Henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Käsittely on lainmukaista, kun sille on olemassa oikeusperuste, asianmukaista ja kohtuullista, kun sitä tehdään tässä mainittujen käsittelyperiaatteiden mukaisesti ja vain silloin kun se on tarpeellista, ja läpinäkyvää, kun rekisteröidylle tarjotaan tietoa omien tietojensa käsittelystä ja mahdollisuus toteuttaa rekisteröidyn oikeuksiaan. Tässä yhtenä välineenä on tietosuojaseloste.
>
> Rekisterinpitäjä vastaa siitä, että henkilötietoja käsitellään oikein ja lainmukaisesti. Rekisterinpitäjän tehtävänä on ohjeistaa ja/tai kouluttaa niin oma henkilökunta kuin rekisterinpitäjän lukuun henkilötietoja käsittelevät ulkopuoliset toimijat niin, että he tietävät, miten henkilötietojen käsittelyä saa tehdä.

Käyttötarkoitussidonnaisuuden periaate:

> Henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten. Ja toisinpäin: henkilötietoja ei saa käyttää kuin siihen käyttötarkoitukseen, johon ne on kerätty.
>
> Jos käyttötarkoitusta halutaan laajentaa, pitää siitä ilmoittaa rekisteröidylle. Jos laajennettu käyttötarkoitus ei enää mahdu aiemman oikeusperusteen piiriin, ei sitä todennäköisesti ole sallittua laajentaa.

Tietojen minimoinnin periaate:

> Henkilötietojen on oltava asianmukaisia, olennaisia ja rajoitettuja niihin tietoihin, jotka ovat tarpeellisia suhteessa niiden käyttötarkoitukseen. Mitään ylimääräisiä henkilötietoja ei saa kerätä varmuuden vuoksi, vaan kaikilla tiedoilla tulee olla merkitystä käyttötarkoitukseen nähden. Henkilötietoja ei myöskään saa käsitellä turhaan.

Täsmällisyyden periaate:

> Henkilötietojen tulee olla oikeellisia ja ajantasaisia, ja rekisteröidyn täytyy voida oikaista epätarkat ja virheelliset tiedot. Tietojen oikaiseminen tai poistaminen pitää tehdä viipymättä.

Säilytyksen rajoittamisen periaate:

> Henkilötietoja ei saa säilyttää siinä muodossa, että niistä tunnistaa henkilön, sen pitempään kuin mikä on tietojenkäsittelyn vuoksi välttämätöntä. Kun tiedot eivät ole enää välttämättömiä, pitää ne joko kokonaan poistaa, tai jos se ei ole mahdollista, pseudonymisoida tai anonymisoida mahdollisuuksien mukaan. Henkilötiedoille pitää määrittää säilytysajat, jonka jälkeen ne automaattisesti joko poistetaan tai käsitellään valitun strategian mukaisesti.
>
> Kun määritellään henkilötietojen säilytysaikaa, on huomioitava mahdolliset kansallisessa lainsäädännössä kuten kirjanpitolaissa tai työnantajan velvoitteissa olevat vaatimukset tietojen säilyttämiselle. Myös EU saattaa asettaa vaatimuksia henkilötietojen säilyttämiselle esimerkiksi hankkeiden rahoittajan ominaisuudessa. Säilytysajoissa ja poistokäytännöissä pitää huomioida myös ne tiedon sijainnit, joihin henkilötietoja on jouduttu monistamaan esimerkiksi tiedonsiirtoihin liittyen. Myös näille sijainneille pitää määrittää säilytysajat, jotka voivat todennäköisesti olla huomattavasti lyhyemmät kuin varsinaisen henkilötiedon säilytysaika.

Eheyden ja luottamuksellisuuden periaate:

> Henkilötietojen käsittelyn turvallisuus pitää varmistaa teknisin keinoin sekä ohjeistuksen ja koulutuksen avulla. Turvallisuus tarkoittaa tietojen suojaamista luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta.

Rekisterinpitäjällä on osoitusvelvollisuus sen suhteen, että näitä käsittelyperiaatteita noudatetaan kaikessa organisaation henkilötietojen käsittelyssä.

B. Toiminta-arkkitehtuuri

Toiminta-arkkitehtuurivaiheessa suunnitellaan tarvittavat muutokset toiminta-arkkitehtuuriin eli prosesseihin ja toimintatapoihin. Tässä vaiheessa tuotetaan toiminnalliset vaatimukset tulevalle tietojärjestelmälle ja kuvataan muun muassa käyttötapaukset. Henkilötietojen käsittelyn osalta pitää ottaa kantaa prosesseihin, joiden avulla toteutetaan rekisteröityjen oikeudet ja myös rekisterinpitäjän velvollisuudet.

Vaiheessa käydään läpi seuraavat asiat sisäänrakennettuun tietosuojaan liittyen:

- Henkilötietojen käsittelyprosessien kuvaaminen
- Mahdollisten tiedonluovutusten määrittely
- Säilytysaikojen päättäminen
- Riskienarvioinnin jatkaminen

Tietosuojan ja henkilötietojen käsittelyn osalta tässä vaiheessa tulisi vastata seuraaviin kysymyksiin:

Tarvitaanko rekisteröidyn suostumus tietojen rekisteröintiin?

#	Otsikko	Input	Output
2.3	Rekisteröidyn on voitava antaa suostumuksensa henkilötietojen rekisteröintiin yksinkertaisella, selkeällä, yksiselitteisellä tavalla	2.1	2.4, 2.5, 2.6
3.3	Rekisterinpitäjän on suostumuksen antamisen yhteydessä mahdollisuuksien mukaan varmistuttava, että rekisteröitävä on vähintään 13-vuotias	2.3	3.3.1, 3.3.2

Toimenpiteet:

- Jos rekisteröinnin oikeusperusteena on rekisteröidyn suostumus, kuvataan suostumuksen antaminen käyttötapaukseksi
  - Vaatii harkitsemaan, onko palvelu ja rekisteröintitapa sen tyyppinen, että on huomioitava mahdollisesti alle 13-vuotiaat rekisteröityjät
  - Kuvataan tietojärjestelmäkuvaukseen, miten varmistutaan rekisteröidyn iästä
- Jos oikeusperusteena ei ole rekisteröidyn suostumus, ei ole tarvetta käsitellä näitä vaatimuksia

Taustatiedot:

- Arkaluonteisten tietojen käsittelystä
- Mitkä ovat lainmukaiset oikeusperusteet henkilötietojen käsittelylle

Mitä oikeuksia rekisteröidyllä on?

#	Otsikko	Input	Output
4.1	Rekisteröidyn on saatava määrätyt tiedot henkilötietojensa käsittelystä helposti ymmärrettävässä, selkeässä muodossa	-	H
4.2	Rekisteröidyn on saatava henkilötiedot antaessaan riittävä tieto rekisteröidyn oikeuksista ja siitä, miten hänen on mahdollista käyttää oikeuksiaan, sekä tietojen säilytysajasta	2.3	C2, 4.9, 4.12, 4.14, 4.25
4.5	Rekisteröidylle on ilmoitettava kuukauden sisällä, jos hänen henkilötietojaan saadaan muualta kuin rekisteröidyltä itseltään	1.6	prosessi
4.7	Rekisteröidyn on saatava tieto siitä, jos kerättyjen henkilötietojen käsittelytarkoitusta laajennetaan	5.2	prosessi
4.9	Rekisteröidyn on voitava ilmoittaa virheellisistä tiedoista tai korjata ne itse	4.2	C2, 4.10
4.12	Rekisteröidyn on voitava pyytää tietojen poistamista tai poistaa ne itse	4.2	C2, 4.13
4.14	Rekisteröidyn on voitava vaatia yksilöidysti henkilötietojen käsittelyn rajoittamista	4.2, 4.16	4.17
4.16	Rekisterinpitäjän on määriteltävä, minkä henkilötietoryhmien käsittelyä on mahdollista rajoittaa	4.15	4.17
4.20	Rekisterinpitäjän on voitavat toimittaa tietojen oikaisu-, poisto- tai rajoituspyyntö kaikille niille tahoille, joille se on luovuttanut kyseisen rekisteröidyn tiedot	4.2	4.19, prosessi
4.25	Rekisteröidyn on voitava vastustaa henkilötietojen käsittelyä tai kieltäytyä automaattisesta päätöksenteosta ja/tai profiloinnista	4.2	4.26
4.28	Rekisterinpitäjän on määritettävä, miten rekisteröity tunnistetaan niillä tiedoilla, jotka hänestä on olemassa	-	prosessi
4.29	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava tunnistaa rekisteröity niillä tiedoilla, jotka hänestä on olemassa	-	C1

Toimenpiteet:

- Kuvataan, miten rekisteröinnin yhteydessä informoidaan rekisteröityä hänen oikeuksistaan ja niiden käyttämisestä
- Kuvataan, miten rekisteröidyn oikeuksiin liittyvät pyynnöt otetaan vastaan: väline, vastaanottaja
- Kuvataan prosessi, jolla rekisteröidyn oikeuspyyntöön vastataan: kuka vastaa, miten toimitaan
- Päätetään, mahdollistetaanko rekisteröidylle omavalvonta eli sähköinen palvelu tietojen katseluun, oikaisuun ja poistamiseen
    - Jos mahdollistetaan, tehdään näistä omat käyttötapauskuvauksensa
    - Jos ei mahdollisteta, kuvataan,
        - miten toimitetaan rekisteröidylle kopio hänen tiedoistaan ja tietosuojaseloste
        - miten hoidetaan tietojen oikaiseminen
        - miten tehdään tietojen poistaminen, jos pyyntö on perusteltu
- Päätetään, miten henkilötietojen käsittelyn rajoittaminen tehdään (henkilötietoryhmät)
    - Kuvataan, miten hoidetaan käsittelyn rajoittamispyyntö
- Päätetään, miten automaattisesta päätöksenteosta kieltäytyminen toteutetaan
    - Kuvataan, miten hoidetaan päätöksenteko ihmisen toimesta
- Kuvataan, miten rekisteröidylle ilmoitetaan, jos saadaan hänen tietojaan toiselta rekisterinpitäjältä
- Kuvataan, miten rekisteröidylle ilmoitetaan käsittelytarkoituksen laajentamisesta
- Kuvataan, miten selvitetään, keille tiedonluovutuksen vastaanottajille pitää ilmoittaa rekisteröidyn tietojen oikaisusta, poistamisesta tai käsittelyrajoituksesta
    - Kuvataan, miten rajoituksista ilmoitetaan
- Kuvataan, miten rekisteröity tunnistetaan ennen tietojen toimittamista tai muiden oikeuksien toteuttamista
- Niiden rekisteröidyn oikeuksien osalta, joita rekisteröidyllä ei kehitettävässä tietojärjestelmässä ole, ei ole tarvetta huomioida siihen liittyviä vaatimuksia tämän jälkeen

Toimenpiteissä hyödynnetään MML:ssa jo käytössä olevia prosesseja ja tapoja parhaan mukaan lisäämällä uuteen tietojärjestelmään liittyvät toimenpiteet samaan prosessiin tai toimintamalliin.

Taustatiedot:

- MML:n prosessi rekisteröidyn oikeuspyyntöjen vastaanottamiseksi ja toteuttamiseksi (PUUTTUU)

Ketkä käsittelevät henkilötietoja?

#	Otsikko	Input	Output
7.1	Henkilötietojen käsittelijällä tulee olla oikeudet vain hänen tehtäviensä kannalta tarpeellisiin tietoihin	-	7.2
7.2	Rekisterinpitäjän on huolehdittava, ettei henkilötietojen käsittelijä pääse käsittelemään tarpeettomia henkilötietoja	7.1	7.7
7.7	Rekisterinpitäjän on huolehdittava, ettei henkilörekisterihin ole oikeuksia kuin heillä, joilla tietojen käsittely kuuluu työtehtäviin	7.2	prosessi

Toimenpiteet:

- Kuvataan henkilötietoja käsittelevät roolit eli eri sidosryhmät
    - Rekisterinpitäjä, sisäinen henkilötietojen käsittelijä, ulkoinen henkilötietojen käsittelijä, rekisteröity
    - Ulkoiset sidosryhmät kuten tiedonluovutusten vastaanottajat, katselukäyttöliittymän käyttäjät
    - Katseluoikeudet, ylläpito-oikeudet, raportointioikeudet, pääkäyttäjäoikeudet, ...
- Kuvataan rajoitukset henkilötietojen käsittelylle
    - Mitkä roolit saavat nähdä ja/tai ylläpitää mitäkin henkilötietoja
- Kuvataan prosessi, jolla käyttöoikeudet myönnetään ja tarkistetaan
    - Ketkä päättävät käyttöoikeuksista, missä työtehtävissä oleville niitä myönnetään
    - Yhteys MML:n käyttövaltuushallinnan tukeen (MML Käyttövaltuudet)

Taustatiedot:

Miten henkilötietojen käsittelyperiaatteet otetaan huomioon?

#	Otsikko	Input	Output
5.1	Rekisterinpitäjän on huomioitava määritetyt käsittelyperiaatteet henkilötietojen käsittelyssä	A	C1
5.5	Rekisterinpitäjän on määriteltävä henkilötietojen säilytysaika mahdollisimman lyhyeksi	1.0	5.8, 5.6
5.8	Rekisterinpitäjän on varmistettava, että määritelty säilytysaika huomioi erillislainsäädännön	5.5	5.6

Toimenpiteet:

- Käydään läpi kuvatut käyttötapaukset ja varmistetaan, että niihin kuvattu henkilötietojen käsittely on käsittelyperiaatteiden mukaista
    - Onko käyttötapauksessa kuvattu käsittely määritetyn käsittelytarkoituksen mukaista?
    - Onko käyttötapauksessa kuvattu käsittely välttämätöntä? Jos se jätetään tekemättä, päästäänkö kuitenkin käsittelytarkoituksen mukaiseen tavoitteeseen?
    - Huomioidaan käyttötapauksissa arkaluonteiset henkilötiedot sekä turvakiellot ja yhteystietojen salassapitopäätökset
    - Saako rekisteröity tarvittavan tiedon henkilötietojensa käsittelystä kuten on säädetty?
    - Ovatko kaikki kuvatut henkilötiedot tarpeellisia vai voidaanko niitä vähentää?
    - Onko henkilötietojen ajantasaisuus huomioitu? Mistä saadaan muuttuneet tiedot?

        - Onko määritelty, ketkä saavat katsella ja/tai muokata henkilötietoja? Onko käyttäjäroolit kuvattu?
- Päätetään henkilötietojen säilytysaika
    - Selvitetään lainsäädännölliset velvollisuudet tietojen säilytykselle
    - Selvitetään organisaation tarpeet tietojen säilytykselle
    - Varmistetaan käsittelyperiaatteiden mukaisuus: Onko säilytysaika määritetty mahdollisimman lyhyeksi?

Taustatiedot:

- Käsittelyperiaatteet tietosuoja-asetuksessa

Mitä tiedonsiirtoja ja -luovutuksia tarvitaan?

#	Otsikko	Input	Output
1.6	Rekisterinpitäjän on pyrittävä hyödyntämään jo kerättyjä henkilötietoja, jos niitä on saatavissa toiselta viranomaiselta	1.0, 2.1, 5.2	C1, C2
6.1	Rekisterinpitäjän on varmistuttava henkilötietojen siirron tai luovutuksen lainmukaisuudesta	-	6.8
6.8	Rekisterinpitäjän on varmistuttava tietonluovutuksen tarpeellisuudesta	6.1	C2
6.10	Rekisterinpitäjän on rekisteröitävä tietopyynnöt asiarekisteriin	6.8	prosessi
6.11	Rekisterinpitäjän on varmistuttava henkilötietojen luovuttamisen kolmansiin maihin lainmukaisuudesta	-	6.8

Toimenpiteet:

- Selvitetään, onko tarvittavat henkilötiedot jo olemassa MML:ssa
    - Onko tiedot tai osa niistä saatavissa jostain muusta MML:n henkilörekisteristä?
    - Jos on, voiko tietoja hyödyntää tässä käsittelytarkoituksessa?
    - Jos ei ole, onko olemassa muuta viranomaista, jolta tiedot voisi saada tiedonluovutuksena?
- Kuvataan käyttötapauksiin, minkälaisia tiedonluovutuksia tarvitaan
    - Varmistetaan, mitä tietoja on oikeus luovuttaa ja kenelle
        - Huomioidaan arkaluonteiset henkilötiedot sekä turvakiellot ja yhteystietojen salassapitopäätökset
    - Kuvataan tiedonluovutusprosessi ja luovutettavat tiedot
        - Toimijat, pyyntöjen rekisteröinti
        - Tiedonluovutuksen periaatteet ja sopimukselliset asiat
        - Kenelle, mihin tarkoitukseen, miten varmistetaan lainmukaisuus ja tarpeellisuus
- Jos on mahdollista, että tietoja luovutetaan EU:n ja ETA:n ulkopuolelle, selvitetään ratkaisun lainmukaisuus

Taustatiedot:

- Tiedonluovutuksista tietosuoja-asetuksessa

Mitä on tietojärjestelmän riskitaso?

#	Otsikko	Input	Output
7.3	Rekisterinpitäjän on huolehdittava henkilötietoja käsittelevän tietojärjestelmän riskiarvioinnista ja sen perusteella tehtävistä toimenpiteistä	A	E

Toimenpiteet:

- Riskienarvioinnin päivittäminen
    - Tarkistetaan, että suunnitellut käyttötapaukset eivät aiheuta riskejä henkilötietojen käsittelylle

Taustatiedot:

- Henkilötietojen turvallisuus

C2. Sovellusarkkitehtuuri

Sovellusarkkitehtuuri-vaiheessa tehdään sovellusarkkitehtuurin määrittely ja kuvataan sovellusarkkitehtuurivaatimukset. Vaiheen lopputuloksena tulisi myös olla lista sovellusarkkitehtuurikomponenteista, joita tarvitaan, ja sovellusarkkitehtuuriperiaatteet, jotka varsinaisessa sovelluskehitysvaiheessa tulee huomioida.

Vaiheessa käydään läpi seuraavat asiat sisäänrakennettuun tietosuojaan liittyen:

- Rekisteröidyn tarvitsemien sovelluspalveluiden kuvaaminen
- Henkilötietojen käsittelijän tarvitsemien sovelluspalveluiden kuvaaminen
- Käyttäjäroolien sovellusoikeuksien kuvaaminen
- Tiedonsiirtojen ja -luovutusten arkkitehtuuriratkaisujen kuvaaminen
- Poistomenettelyjen kuvaaminen

Tietosuojan ja henkilötietojen käsittelyn osalta tässä vaiheessa tulisi vastata seuraaviin kysymyksiin:

Käsitelläänkö henkilötunnusta?

#	Otsikko	Input	Output
1.3	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta käsitellä käyttöliittymässä ilman erityistä tarvetta	1.2	sovkeh
1.4	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta merkitä tulosteisiin ilman erityistä tarvetta	1.2	sovkeh
1.5	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta luovuteta ilman lakisääteistä oikeutta sen luovuttamiseen	1.2	sovkeh

Toimenpiteet:

- Käyttöliittymäsuunnittelussa on pidettävä periaatteena, ettei henkilötunnusta esitetä näytölle, ellei se ole erityisesti tarpeen
  - Samoin tulosteiden suunnittelussa on pidettävä periaatteena, ettei henkilötunnusta tulosteta asiakirjaan tai raportille, ellei se ole erityisesti tarpeen
  - Käyttöliitymässä henkilötunnuksen voi mahdollisesti peittää käyttäjäroolin mukaan
  - Asiakirjoista voi tarvittaessa olla olemassa kaksi versiota, hetullinen ja hetuton
- Rajapintasuunnittelussa on pidettävä periaatteena, ettei henkilötunnusta automaattisesti luovuteta muiden henkilötietojen mukana vastaanottajalle
  - Ennen tiedonluovutuksen toteutusta tulee käydä läpi, onko henkilötunnuksen luovutukseen oikeutta
  - Rajapinnoista voi tarvittaessa olla olemassa kaksi versiota, hetullinen ja hetuton

Taustatiedot:

- Henkilötunnuksen käsittely

Mitä toimintoja rekisteröity tarvitsee?

#	Otsikko	Input	Output
2.2	Rekisteröidyn on saatava riittävät tiedot henkilötietojen käsittelystä henkilötietojen rekisteröintiin suostumuksen tueksi	2.3	E
2.3	Rekisteröidyn on voitava antaa suostumuksensa henkilötietojen rekisteröintiin yksinkertaisella, selkeällä, yksiselitteisellä tavalla	B	E
2.6	Rekisteröidyn on voitava peruuttaa suostumuksensa yhtä helposti kuin on sen antanut	2.3	E
3.3	Rekisterinpitäjän on suostumuksen antamisen yhteydessä mahdollisuuksien mukaan varmistuttava, että rekisteröitävä on vähintään 13-vuotias	2.3	E
3.3.1	Rekisterinpitäjän on ilmaistava palvelun ikäraja selkeästi suostumuksen antamisen yhteydessä	3.3	E
3.3.2	Rekisteröitävän huoltajalle on tarjottava mahdollisuus antaa suostumus tai valtuutus, jos rekisteröitävä on alle 13-vuotias	3.3	E
4.1	Rekisteröidyn on saatava määrätyt tiedot henkilötietojensa käsittelystä helposti ymmärrettävässä, selkeässä muodossa	2.1	E
4.2	Rekisteröidyn on saatava henkilötiedot antaessaan riittävä tieto rekisteröidyn oikeuksista ja siitä, miten hänen on mahdollista käyttää oikeuksiaan, sekä tietojen säilytysajasta	2.1	E
4.3	Rekisteröidyn on voitava antaa tarvittavat tiedot rekisteröintiä varten	2.1	E
4.9	Rekisteröidyn on voitava ilmoittaa virheellisistä tiedoista tai korjata ne itse	4.2	E
4.12	Rekisteröidyn on voitava pyytää tietojen poistamista tai poistaa ne itse	4.2	E
9.1	Rekisterinpitäjän on liitettävä tietosuojaseloste rekisteröidyille tarjottaviin palveluihin näiden nähtäväksi	4.1	E

Toimenpiteet:

- Suunnitellaan rekisteröidylle mahdollisuus rekisteröityä, jos kyse on suostumukseen perustuvasta rekisteröinnistä

        - Liitetään rekisteröinnin yhteyteen tietosuojaseloste
        - Liitetään rekisteröinnin yhteyteen tiedon rekisteröidyn oikeuksista ja niiden käyttämisestä
        - Liitetään rekisteröinnin yhteyteen selvästi tieto oikeudesta vastustaa käsittelyä
        - Määritetään, miten rekisteröity antaa suostumuksensa rekisteröintiin
        - Määritetään, miten varmistetaan rekisteröidyn ikä: esitetäänkö ikäraja vai vaaditaanko huoltajan suostumus alle 13-vuotiailta?
- Suunnitellaan rekisteröidylle mahdollisuus peruuttaa suostumuksensa rekisteröintiin
    - Määritetään, miten tiedot poistetaan suostumuksen peruuttamisen jälkeen
- Määritellään, voiko rekisteröity itse poistaa omat tietonsa
- Määritellään, voiko rekisteröity itse oikaista tietonsa

Rekisteröinnissä ja suostumuksen antamisessa sekä tarvittavien rekisteröidyn oikeuksien esittämisessä tulee käyttää MML:n yhteisiä menettelyitä, jos sellaisia on olemassa

Taustatiedot:

- Rekisteröidyn oikeudet

Mitä toimintoja henkilötietojen käsittelijä tarvitsee?

#	Otsikko	Input	Output
3.2.1	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä yhteystietojen salassapitopäätös tietojärjestelmään	3.2	sovkeh
4.4	Rekisterinpitäjän on voitava tunnistaa, mistä rekisteröidyn henkilötiedot on saatu	4.5	prosessi
4.5	Rekisteröidylle on ilmoitettava kuukauden sisällä, jos hänen henkilötietojaan saadaan muualta kuin rekisteröidyltä itseltään	1.6	prosessi
4.8	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä luettavassa, sähköisessä muodossa nopeasti ja luotettavasti	C1	sovkeh
4.10	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava korjata virheelliset tiedot	4.9	sovkeh
4.13	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa henkilötiedot tarvittaessa	4.12	sovkeh
4.17	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä rekisteröidyn tietoihin kyseisten tietojen käsittelyrajoitus	4.14	sovkeh
4.18	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava ohittaa käsittelyrajoitetut henkilötiedot	4.17	sovkeh
4.19	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan tietojärjestelmästä tieto siitä, kenelle rekisteröidyn tiedot on luovutettu	6.7	sovkeh
4.26	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä automaattisen päätöksenteon ja profiloinnin kielto rekisteröidyn tietoihin	4.25	sovkeh
4.27	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava käsitellä manuaalisesti automaattisesta päätöksenteosta estetyt henkilötiedot	4.26	sovkeh
4.29	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava tunnistaa rekisteröity niillä tiedoilla, jotka hänestä on olemassa	C1	sovkeh

Toimenpiteet:

- Määritellään, miten yhteystietojen salassapitopäätös merkitään tietojärjestelmään
    - Saadaanko tieto toisesta henkilörekisteristä?
    - Salassapitopäätös kuten myös turvakielto tulisi olla merkittynä henkilötietojen perustietoihin (master dataan), josta se on kaikkien muiden MML:n henkilörekisterien käytettävissä
- Määritellään, miten merkitään, mistä rekisteröidyn tiedot on saatu
    - Mahdollisesti riittää asian kuvaaminen tietosuojaselosteeseen, eikä tarvita tiedon tallentamista tiedonluovutuksen yhteydessä
- Jos rekisteröidyn tietoja saadaan toiselta rekisterinpitäjältä
    - Selvitetään, onko MML:lla ilmoitusvelvollisuus rekisteröidylle
    - Jos on, määritellään, miten ilmoitetaan rekisteröidylle tietojen saamisesta
        - Vaatii todennäköisesti puoliautomaattisen prosessin, jossa tuotetaan tiedot muualta saaduista henkilötiedoista ja toimitetaan ne prosessille, joka huolehtii ilmoittamisesta
        - Vaatii myös rekisteriin merkinnän siitä, jos tiedot on jo toimitettu
    - Ilmoitus tulee tehdä joko ensimmäisen kontaktin yhteydessä, kun rekisteröidyn tiedot luovutetaan eteenpäin kolmannelle osapuolelle ensimmäistä kertaa, tai viimeistään kuukauden sisällä tietojen vastaanottamisesta toiselta rekisterinpitäjältä
- Kuvataan, miten henkilörekisteristä tuotetaan rekisteröidyn tiedot luovutusta varten
    - Miten tuotetaan kopio tiedoista luettavassa, selvässä muodossa rekisteröidyn pyytäessä niitä joko sähköisessä tai paperisessa muodossa
- Kuvataan, miten rekisteröidyn tiedot voidaan tarvittaessa oikaista
    - Huomioitava toisesta henkilörekisteristä tai toiselta rekisterinpitäjältä monistettavat tiedot korjaaminen alkuperäiseen lähteeseen
- Jos rekisteröidyn henkilötiedot on sallittua poistaa pyynnöstä, kuvataan, miten poisto tehdään
- Jos rekisteröidyllä on oikeus rajoittaa tai vastustaa käsittelyä, kuvataan miten rajoittaminen ja/tai vastustaminen tietojärjestelmään merkitään
    - Huomioitava muissa toiminnallisuuksissa, miten rajoitetut tiedot ohitetaan tietojärjestelmässä
- Määritellään, miten rekisteröidyn käyttämästä oikaisu-, poisto- tai rajoitusvaatimuksesta ilmoitetaan niille, joille rekisteröidyn tiedot on luovutettu
    - Miten tuotetaan lokista tiedot siitä, kenelle tiedot on luovutettu
        - Tiedot pitää voida luovuttaa myös rekisteröidylle itselleen, jos tämä sitä pyytää
    - Mikä prosessi hoitaa ilmoittamisen
- Määritellään, miten automaattisen päätöksenteon tai profiloinnin kielto merkitään tietojärjestelmään
    - Määritellään, miten henkilötietojen käsittelijä voi tehdä päätöksen automaattisen päätöksenteon sijaan
    - Määritellään, miten henkilötietojen käsittelijä saa tiedon odottavasta päätöksenteosta
- Kuvataan, miten rekisteröity tunnistetaan ennen tietojen luovuttamista

Taustatiedot:

- Rekisteröidyn oikeudet
- Ohje yhteystietojen salassapitopäätöksen käsittelystä

Mitä tiedonsiirtoja ja -luovutuksia tarvitaan?

#	Otsikko	Input	Output
1.6	Rekisterinpitäjän on pyrittävä hyödyntämään jo kerättyjä henkilötietoja, jos niitä on saatavissa toiselta viranomaiselta	1.0	sovkeh
5.4	Rekisterinpitäjän on mahdollisuuksien mukaan huolehdittava rekisteröidyn tietojen ajantasaisuudesta tietoteknisin keinoin	1.6	sovkeh
6.2	Rekisterinpitäjän on huolehdittaa henkilötietojen näkyvyyden rajoittamisesta soveltuvin osin	6.1	sovkeh
6.5	Rekisterinpitäjän on toteutettava tietovarantonsa niin, että myös muut viranomaiset voivat niitä hyödyntää	6.1	sovkeh
6.6	Rekisterinpitäjän on voitava tunnistaa luovutettujen tietojen vastaanottaja	6.1	sovkeh
6.7	Rekisterinpitäjän on kerättävä lokia tiedonluovutuksista	6.1	sovkeh
6.9	Rekisterinpitäjän on huolehdittava siitä, ettei käyttöliittymässä ole näkyvissä tarpeettomia tietoja	6.2	sovkeh

Toimenpiteet:

- Jos rekisteröidyn tietoja on mahdollista saada toiselta rekisterinpitäjältä, kuvataan tiedon vastaanotto ja käsittely
  - Ajantasaisuuden huomioon ottaminen
- Jos rekisteröidyn tietoja käytetään toisesta MML:n henkilörekisteristä, kuvataan yhteys rekisteriin
- Jos rekisteröidyn tietoja monistetaan toisesta MML:n henkilörekisteristä, kuvataan tiedonsiirto ja käsittely
  - Ajantasaisuuden huomioon ottaminen
- Jos rekisteröidyn tietoja monistetaan toiseen MML:n henkilörekisteriin, kuvataan tietojen poiminta ja tiedonsiirto
  - Siirretään vain tarvittavat tiedot
  - Huomioidaan rekisteröityjen, joilla on turvakielto tai yhteystietojen salassapitopäätös, käsittely tiedonluovutuksissa
- Jos rekisteröidyn tietoja annetaan pyydettäessä rajapinnan kautta MML:n muille järjestelmille, kuvataan rajapinta ja tietojen poiminta
  - Rajataan tiedot vain tarvittaviin tietoihin
- Jos rekisteröidyn tietoja luovutetaan kolmannelle osapuolelle, kuvataan rajapinta ja tietojen poiminta tai muu tiedonsiirtomenettely
  - Varmistutaan siitä, ettei luovuteta kuin välttämättömät tiedot, joiden luovuttamiseen on oikeus
  - Huomioidaan arkaluonteiset henkilötiedot sekä turvakiellot ja yhteystietojen salassapitopäätökset
  - Luovutuksen vastaanottajasta on varmistuttava teknisin keinoin, jotta tietoja ei luovuteta väärälle vastaanottajalle
  - Tietopyynnön tekijästä on varmistuttava teknisin keinoin, mieluummin henkilö- kuin organisaatiotasolla, jotta tietoja ei luovuteta oikeudettomalle vastaanottajalle
  - Jokainen tiedonluovutus, josta rekisteröity on tunnistettavissa, on lokitettava, jotta voidaan tarvittaessa tuottaa ulos tiedot tiedonluovutuksen saajista
- Jos kolmannelle osapuolelle toteutetaan katselukäyttöliittymä henkilörekisteriin, varmistutaan siitä, ettei käyttöliittymässä näytetä ylimääräisiä tietoja rekisteröidystä

Taustatiedot:

- Tietojen siirto ja luovuttaminen
- Väestötietojärjestelmän tiedot

Miten huolehditaan henkilörekisterin turvallisuudesta?

#	Otsikko	Input	Output
3.2	Rekisterinpitäjän on rajoitettava arkaluonteisten henkilötietojen käsittelyä riittävin tietoteknisin ratkaisuin	3.1	sovkeh
5.7	Rekisterinpitäjän on suojattava henkilötiedot mahdollisimman hyvin asiattomalta pääsyltä	5.3	E
5.7.1	Rekisterinpitäjän on suojattava henkilötietojen käsittely soveltuvin käyttövaltuuksin	5.3	E
7.1	Henkilötietojen käsittelijällä tulee olla oikeudet vain hänen tehtäviensä kannalta tarpeellisiin tietoihin	B	sovkeh
7.2	Rekisterinpitäjän on huolehdittava, ettei henkilötietojen käsittelijä pääse käsittelemään tarpeettomia henkilötietoja	B	sovkeh
7.7	Rekisterinpitäjän on huolehdittava, ettei henkilörekisterihin ole oikeuksia kuin heillä, joilla tietojen käsittely kuuluu työtehtäviin	B	prosessi
7.8	Rekisterinpitäjän on kerättävä lokia tietojärjestelmän käytöstä	7.3	sovkeh
8.3	Rekisterinpitäjän on huolehdittava henkilötietojen käsittelyn lokittamisesta, jotta pystytään selvittämään loukatut rekisteröidyt ja henkilötiedot	7.3	sovkeh
8.6	Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla tietoturvaloukkaukset olisi mahdollista havaita	7.3	sovkeh

Toimenpiteet:

- Rajoitetaan pääsyä henkilötietoihin käyttövaltuuksin

- Rajoitetaan henkilötietojen näkyvyyttä riittävästi käyttöoikeuksiltaan eroteltujen käyttäjäroolien avulla
    - Tietojärjestelmän toiminnot järjestetään käyttäjäroolien perusteella ryhmiin, joihin saa oikeuden vain, jos tarvitsee toimintoa työtehtävissä
    - Henkilötietojen näkyvyyttä rajoitetaan käyttäjäroolien mukaan
    - Arkaluonteisten henkilötietojen käsittelylle tarvitaan oma roolinsa, johon käyttäjä on oikeutettu vain, jos työtehtävät sitä vaativat
    - Huomioidaan rekisteröityjen, joilla on turvakielto tai yhteystietojen salassapitopäätös, tietojen näkyvyys ja käsittely käyttövaltuuksin
- Täsmennetään käyttövaltuuksien hallintaprosessia
    - Kuvataan vastuut ja oikeuksien tarkastusmenettelyt
- Kuvataan järjestelmään kirjautumisen ja sieltä uloskirjautumisen lokittaminen
- Kuvataan henkilötietojen käsittelyn lokittaminen
    - Tietyn rekisteröidyn henkilön tietojen katselu
    - Tietyn rekisteröidyn henkilön tietojen muuttaminen, mahdollisuuksien mukaan myös muutettu tieto
    - Tietyn rekisteröidyn henkilön tietojen poistaminen
    - Sähköisessä tiedonluovutuksessa luovutettujen henkilöiden tiedot (tai henkilö ja tiedonluovutus (tuote), jonka perusteella voidaan tarvittaessa päätellä luovutetut tiedot) sekä vastaanottaja/tietopyynnön tekijä
    - Säilytysajan jälkeen tehtävä tietojen poisto
    - Säilytysajan jälkeen tehtävä tietojen pseudonymisointi
    - Säilytysajan jälkeen tehtävä tietojen anonymisointi, kun tiedot edelleen säilytetään erityisiä tarkoituksia varten

Tietosuojaprojektissa tehdyn määrittelyn mukaan hakua, jonka tuloksena saadaan tulosjoukko, ei ole tarvetta lokittaa. Jos tulosjoukosta kuitenkin avataan tietyn rekisteröidyn tiedot, pitää tämä lokittaa. Tulosjoukosta on huolehdittava, ettei siinä näytetä kuin mahdollisimman vähäiset tiedot rekisteröidyistä.

Taustatiedot:

- Käyttövaltuushallinnasta teknologiakäsikirjassa
- Lokienhallinnasta ASHAssa

Miten tiedot poistetaan säilytysajan jälkeen?

#	Otsikko	Input	Output
5.6	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa tai anonymisoida henkilötiedot säilytysajan päätyttyä	5.5	sovkeh
5.9	Rekisterinpitäjän on tiedettävä, minne kaikkialle henkilötieto on tallennettu ja monistettu	5.5	sovkeh
5.10	Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja	5.9	sovkeh
5.11	Rekisterinpitäjän on huolehdittava henkilötietojen minimoinnista, jos henkilötietoja säilytetään erityisiä käsittelytarkoituksia varten	5.6	sovkeh

Toimenpiteet:

- Määritetään poistomenettelyt
    - Kuvataan, poistetaanko tiedot heti säilytysajan täyttymisen jälkeen, jolloin poiston täytyy tapahtua päivittäin, vai esimerkiksi kerran vuodessa
    - Kuvataan fyysiset sijainnit, joissa henkilötietoja on
    - Kuvataan kunkin fyysisen sijainnin säilytysajat
        - Välitallennuspaikkojen kuten levyjakojen säilytysaikojen tulee olla lyhyet, tietoja ei saa säilyttää kuin sen aikaa kuin se on välttämätöntä
    - Kuvataan kustakin fyysisestä sijainnista poistettavat tiedot ja poistotavat
        - Fyysinen poistaminen, tietojen maskaaminen, tietojen pseudonymisointi, tietojen anonymisointi
    - Jos tiedot halutaan edelleen säilyttää erityisiä käsittelytarkoituksia varten, on suunniteltava arkistointimenetelmät
        - Henkilötietojen minimointi: anonymisointi tai vähintään pseudonymisointi
    - Muistettava lokittaa poistettavat tiedot

Taustatiedot:

- Lokienhallinnan dokumentaatio

Liite C Sovelluskehitysvaiheen tietosuojaohje

Maanmittauslaitokselle tutkielman lopputuloksena toteutetun tietosuojaohjeiston sivu Sovelluskehitysvaihe on esitetty tässä liitteessä. Sivulle on kerätty ne sisäänrakennetun tietosuojan vaatimukset, jotka tulee toteuttaa sovelluskehitysprojektissa. Vaatimuksiin liittyvä arkkitehtuurimäärittely on tehty ennen tämän vaiheen käynnistymistä.

Vaatimukset on ryhmitelty Maanmittauslaitoksessa käytössä olevan teknologiakäsikirjan [22] mukaisesti. Kuhunkin vaatimukseen tai joukkoon vaatimuksia on liitetty ohje siitä, miten kyseistä vaatimusta tulee käsitellä, toisin sanoen mitä siihen liittyen pitää sovelluskehityksen aikana ottaa huomioon tai toteuttaa sovellukseen. Lisäksi vaatimustaulukoiden yhteyteen on lisätty hyperlinkkejä Maanmittauslaitoksen sisäiseen ohjeistukseen.

Sovelluskehitysvaihe

Sovelluskehitysvaiheessa huomioitavat vaatimukset on järjestetty teknologiakäsikirjan otsikoinnin mukaisesti.

Sovelluskehitysvaiheen aikana ja päätteeksi tulee vielä kerran tehdä riskienarviointia ja tarkistaa, että aiemmissa vaiheissa A, B ja E löydettyjen riskien ehkäisemiseksi on toteutettu riittävät toimenpiteet ja ettei sovelluskehitysvaiheessa ole löytynyt uusia riskejä henkilötietojen käsittelylle. Ohjeistus riskienarvioinnin tekemiseksi on sivulla Henkilötietojen turvallisuuden varmistaminen.

Yhteiset tukipalvelut

Käyttövaltuushallinta

#	Otsikko	Käsittely
5.7.1	Rekisterinpitäjän on suojattava henkilötietojen käsittely soveltuvin käyttövaltuuksin	Käyttäjäroolit työtehtävien mukaan Ulkoisten käyttäjien käyttöoikeudet esim. rekisteröidyt, tiedonluovutuksen vastaanottajat, ulkoiset ylläpitäjät, sovelluskehittäjät KVH-palveluiden (käyttövaltuushallinta, pääsynhallinta, tunnistaminen) käyttö sovellusarkkitehtuurissa
6.2	Rekisterinpitäjän on huolehdittaa henkilötietojen näkyvyyden rajoittamisesta soveltuvin osin	
7.2	Rekisterinpitäjän on huolehdittava, ettei henkilötietojen käsittelijä pääse käsittelemään tarpeettomia henkilötietoja	
7.7	Rekisterinpitäjän on huolehdittava, ettei henkilörekisterihin ole oikeuksia kuin heillä, joilla tietojen käsittely kuuluu työtehtäviin	

Käyttövaltuushallinnasta teknologiakäsikirjassa

Käyttövaltuushallinta Confluencessa

Lokienhallinta

#	Otsikko	Käsittely
6.7	Rekisterinpitäjän on kerättävä lokia tiedonluovutuksista	Jokainen tiedonluovutus, josta rekisteröity on tunnistettavissa, lokitetaan
7.8	Rekisterinpitäjän on kerättävä lokia tietojärjestelmän käytöstä	Jokainen onnistunut ja epäonnistunut sisään- ja uloskirjautuminen lokitetaan
8.3	Rekisterinpitäjän on huolehdittava henkilötietojen käsittelyn lokittamisesta, jotta pystytään selvittämään loukatut rekisteröidyt ja henkilötiedot	Jokainen yksittäisen rekisteröidyn katselu, tallennus, muuttaminen ja poisto lokitetaan Jokainen poistoajossa poistettava tieto lokitetaan
8.6	Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla tietoturvaloukkaukset olisi mahdollista havaita	LOKKI-palvelun käyttö Valvonnat lokitapahtumiin poikkeamien varalta
8.7	Rekisterinpitäjän on pyrittävä määrittelemään ja löytämään tietovarantoihinsa tehtävät poikkeavat haut	

Lokien kehittäjäohje #271623

Varmistuspalvelu

#	Otsikko	Käsittely
5.10	Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja	Varmistusten säilytysaika Kuvattava, miten poistetaan varmistusten oton jälkeen kannasta poistetut henkilötiedot, jos kanta joudutaan palauttamaan varmistuksista (jatkuvuudenhallinta)
8.4	Rekisterinpitäjän on salattava tietovälineille tallennettu data	?

Valvontajärjestelmät

#	Otsikko	Käsittely

8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin	Valvontaan koputtelut ja yritykset päästä palveluun vääristä osoitteista
8.6	Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla tietoturvaloukkaukset olisi mahdollista havaita	Valvonnat palvelimiin ja tietoliikenteeseen /palomuureihin poikkeamien varalta

ICT-infrastruktuuri

Ympäristöt

#	Otsikko	Käsittely
5.7.2	Rekisterinpitäjän on suojattava henkilötietojen käsittely-ympäristö soveltuvin teknisin ratkaisuin ja käyttövaltuuksin	Käyttöoikeudet: sisäiset asiantuntijat, ulkoiset sovelluskehittäjät ja infran ylläpitäjät • Huomioitava mahdollinen tuotantodatan käyttö kehitys- ja testiympäristöissä
5.9	Rekisterinpitäjän on tiedettävä, minne kaikkialle henkilötieto on tallennettu ja monistettu	Tietojen fyysisten sijaintien dokumentointi, tietovirtakuvaukset Eri ympäristöjen (kehitys, testi, tuotanto) henkilötietojen säilytysajat ja poistomenettelyt Eri tietovarantojen (kannat, levyjaot, muut säilytyspaikat) henkilötietojen säilytysajat ja poistomenettelyt
5.10	Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja	
8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin	Palomuurisuojaukset, verkkosegmentöinnit
8.4	Rekisterinpitäjän on salattava tietovälineille tallennettu data	?

Tietokannat

#	Otsikko	Käsittely
5.7.2	Rekisterinpitäjän on suojattava henkilötietojen käsittely-ympäristö soveltuvin teknisin ratkaisuin ja käyttövaltuuksin	Käyttöoikeudet: sisäiset asiantuntijat, ulkoiset sovelluskehittäjät ja infran ylläpitäjät • Huomioitava mahdollinen tuotantodatan käyttö kehitys- ja testiympäristöissä
5.9	Rekisterinpitäjän on tiedettävä, minne kaikkialle henkilötieto on tallennettu ja monistettu	Tietojen fyysisten sijaintien dokumentointi, tietovirtakuvaukset Poistomenettelyt kaikkiin sijainteihin Kehitys- ja testiympäristöissä käytettävien henkilötietojen toteutusmenettelyt • Tietojen sotkemisen tai pseudonymisoinnin algoritmit • Jos käytetään tuotantodataa kehityksessä ja/tai testissä, huomioitava poistomenettelyissä
5.10	Rekisterinpitäjän on varmistettava, että poistokäytännöt koskevat kaikkia henkilötiedon säilytyspaikkoja	
8.7	Rekisterinpitäjän on pyrittävä määrittelemään ja löytämään tietovarantoihinsa tehtävät poikkeavat haut	Valvonnat ja/tai lokitukset suoriin tietokantahakuihin, jos mahdollista

Sovellusarkkitehtuuri

Integraatioarkkitehtuuri

#	Otsikko	Käsittely

1.6	Rekisterinpitäjän on pyrittävä hyödyntämään jo kerättyjä henkilötietoja, jos niitä on saatavissa toiselta viranomaiselta	Hyödynnetään toisen rekisterinpitäjän tietoja, jos se tuottaa ajantasaiset tiedot (esim. VTJ, YTJ, VERO, ulosottoviranomainen) Hyödynnetään muita MML:n henkilörekistereitä, jos tiedot on jo olemassa Huomioitava häiriötilanteet • miten toimitaan, jos toisen rekisterinpitäjän tiedot ovat virheellisiä rinnalle korvaavan tiedon tallennusmahdollisuus? • miten toimitaan, jos toisen rekisterinpitäjän tiedot eivät ole saatavilla esim. tietoliikennehäiriön vuoksi? • miten toimitaan, jos MML:n oma palvelu ei vastaa?
5.4	Rekisterinpitäjän on mahdollisuuksien mukaan huolehdittava rekisteröidyn tietojen ajatasaisuudesta tietoteknisin keinoin	Tietojen automaattipäivittymisen frekvenssi, ajastukset
6.5	Rekisterinpitäjän on toteutettava tietovarantonsa niin, että myös muut viranomaiset voivat niitä hyödyntää	Arvioidaan tarvetta muiden viranomaisten tai muiden MML:n prosessien käyttöön ja otetaan tämä huomioon rakenteissa ja rajapinnoissa
6.6	Rekisterinpitäjän on voitava tunnistaa luovutettujen tietojen vastaanottaja	Tiedonluovutuspyynnöt, tiedettävä kuka pyytää mieluummin henkilö- kuin organisaatiotasolla
6.10	Rekisterinpitäjän on rekisteröitävä tietopyynnöt asiarekisteriin	Vastaanottajasta varmistuminen ennen tiedon luovuttamista Pyynnön merkitseminen Asianhallintaan / diaariin / lokiin
8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin	Rajapinnat tietoturvallisiksi, ettei ole mahdollisuutta saada tiedonluovutusta aikaiseksi virheellisellä pyynnöllä
8.6	Rekisterinpitäjän on pyrittävä määrittelemään mahdolliset poikkeamat tietojenkäsittely-ympäristössään, joiden avulla tietoturvaloukkaukset olisi mahdollista havaita	Valvonnat rajapintoihin poikkeamien varalta

Sovelluskehitys

Käyttöliittymä

#	Otsikko	Käsittely
1.3	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta käsitellä käyttöliittymässä ilman erityistä tarvetta	Henkilötunnus näkyviin vain, jos rekisteröidyn tunnistaminen on tarpeellista Arkaluonteiset henkilötiedot näkyviin vain, jos liittyvät työtehtäviin • Turvakiellon ja/tai yhteystietojen salassapitopäätöksen omaavan henkilön henkilötietoja ei saa käsitellä kuin erikseen määritetyt henkilöt Erilliset näytöt/välilehdet/haitarit muille tiedoille ja arkaluonteisille henkilötiedoille ml. hetu • Turvakielto- ja salassapitopäätöshenkilöiden tiedot erillisille näytöille, jos heidän yhteystietojaan on henkilörekisterissä Käsittelystä rajoitettujen tietojen näkymisen estäminen, ellei tieto ole tarpeen käsittelijälle • Jos käyttäjä saa tiedot nähdä, oltava näytöllä tieto rajoituksesta Käyttäjäroolitus, kaikki eivät saa käsitellä kaikkea
3.2	Rekisterinpitäjän on rajoitettava arkaluonteisten henkilötietojen käsittelyä riittävin tietoteknisin ratkaisuin	
4.18	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava ohittaa käsittelyrajoitetut henkilötiedot	
6.2	Rekisterinpitäjän on huolehdittaa henkilötietojen näkyvyyden rajoittamisesta soveltuvin osin	
6.9	Rekisterinpitäjän on huolehdittava siitä, ettei käyttöliittymässä ole näkyvissä tarpeettomia tietoja	
2.2	Rekisteröidyn on saatava riittävät tiedot henkilötietojen käsittelystä henkilötietojen rekisteröintiin suostumuksen tueksi	Rekisteröidyn kirjautumisen yhteyteen tietosuojaseloste ja tiedot rekisteröidyn oikeuksista
4.1	Rekisteröidyn on saatava määrätyt tiedot henkilötietojensa käsittelystä helposti ymmärrettävässä, selkeässä muodossa	
4.2	Rekisteröidyn on saatava henkilötiedot antaessaan riittävä tieto rekisteröidyn oikeuksista ja siitä, miten hänen on mahdollista käyttää oikeuksiaan, sekä tietojen säilytysajasta	
9.1	Rekisterinpitäjän on liitettävä tietosuojaseloste rekiseröidyille tarjottaviin palveluihin näiden nähtäväksi	
2.3	Rekisteröidyn on voitava antaa suostumuksensa henkilötietojen rekisteröintiin yksinkertaisella, selkeällä, yksiselitteisellä tavalla	Rekisteröidylle tallennusnäyttö rekisteröintiin suostumisen vahvistamiseen: vaaditaan kuittaus (ruksi ja ok), että on ymmärtänyt, että tiedot rekisteröidään

3.3	Rekisterinpitäjän on suostumuksen antamisen yhteydessä mahdollisuuksien mukaan varmistuttava, että rekisteröitävä on vähintään 13-vuotias	Miten reagoidaan alle 13-vuotiaisiin rekisteröityjiin? Ikäraja vai huoltajan hyväksyminen? Vaatii vahvan tunnistautumisen?
2.6	Rekisteröidyn on voitava peruuttaa suostumuksensa yhtä helposti kuin on sen antanut	Rekisteröidyn kirjautumisen yhteyteen mahdollisuus peruuttaa rekisteröinnin suostumus tietojen poisto samassa yhteydessä tai C2:ssa määritetyn mukaisesti
4.3	Rekisteröidyn on voitava antaa tarvittavat tiedot rekisteröintiä varten	Rekisteröidylle tallennusnäyttö tietojen luovuttamista varten
4.9	Rekisteröidyn on voitava ilmoittaa virheellisistä tiedoista tai korjata ne itse	Rekisteröidylle tallennusnäyttö tietojen oikaisemista ja mahdollisesti myös poistamista varten
4.12	Rekisteröidyn on voitava pyytää tietojen poistamista tai poistaa ne itse	Voidaan korvata henkilötietojen käsittelijän ylläpitotoiminnolla, jolloin rekisteröity tekee oikaisu- tai poistopyynnön palvelussa olevan ohjeen mukaan
8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin	Rekisteröidyn käyttöliittymän tietoturvallisuus ja porsaanreikien tukkiminen, ei jätetä mahdollisuuksia esim. sql-injektiolle
3.2.1	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä yhteystietojen salassapitopäätös rekisteröidyn tietoihin	Henkilötietojen käsittelijälle ylläpitonäyttö seuraaviin rekisteröidyn tietojen muutoksiin: • yhteystietojen salassapitopäätöksen merkitsemiseen • tietojen oikaisemiseen • miten toimitaan, jos virheelliset tiedot tulevat toiselta rekisterinpitäjältä rinnakkaisen tiedon tallennusmahdollisuus tai automaattipäivityksen esto? • mahdollisesti tietojen poistamiseen • tietojen käsittelyn vastustamisen ja mahdollisesti rajoittamisen merkitsemiseen • automaattisen päätöksenteon eston merkitsemiseen • profiloinnin kiellon eston merkitsemiseen Rekisteröidyn tunnistamiseen tarvittavien tietojen näyttäminen näytöllä Käyttäjäroolitus, kaikki eivät saa käsitellä kaikkea
4.10	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava korjata virheelliset tiedot	
4.13	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa henkilötiedot tarvittaessa	
4.17	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä rekisteröidyn tietoihin kyseisten tietojen käsittelyrajoitus	
4.26	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava merkitä automaattisen päätöksenteon ja profiloinnin kielto rekisteröidyn tietoihin	
4.29	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava tunnistaa rekisteröity niillä tiedoilla, jotka hänestä on olemassa	

Tulosteet ja tiedonluovutukset

#	Otsikko	Käsittely
1.4	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta merkitä tulosteisiin ilman erityistä tarvetta	Henkilötunnus vain tulosteisiin, jotka annetaan rekisteröidylle itselleen
1.5	Rekisterinpitäjän on huolehdittava, ettei henkilötunnusta luovuteta ilman lakisääteistä oikeutta sen luovuttamiseen	Henkilötunnus tiedonluovutuksiin vain, jos se on välttämätöntä. Silloinkin on varmistuttava siitä, että luovuttamiseen on lakisääteinen oikeus.
4.8	Rekisterinpitäjän tai henkilötietojen käsittelijän on pystyttävä tuottamaan rekisteröidyn henkilötiedot tietojärjestelmästä luettavassa, sähköisessä muodossa nopeasti ja luotettavasti	Pdf-tuloste rekisteröidyn tiedoista henkilörekisterissä, oltava toimitettavissa rekisteröidylle sekä sähköisesti että kirjepostina Yhdistäminen muiden henkilörekisterien tietoihin?
4.19	Rekisterinpitäjän tai henkliötietojen käsittelijän on pystyttävä tuottamaan tietojärjestelmästä tieto siitä, kenelle rekisteröidyn tiedot on luovutettu	Raportti tiedonluovutuksen vastaanottajista, oltava tuotettavissa lokitiedoista tarvittaessa Vastaanottajien yhteystiedot, mistä saatavissa? Vastaanottajien rekisteröinti?
6.10	Rekisterinpitäjän on rekisteröitävä tietopyynnöt asiarekisteriin	Rekisteröityjen pyynnöt oikeuksien käyttämiseksi merkittävä Asianhallintaan
8.7	Rekisterinpitäjän on pyrittävä määrittelemään ja löytämään tietovarantoihinsa tehtävät poikkeavat haut	Valvonta tiedonhakuihin

Tietosisältö

#	Otsikko	Käsittely
2.4	Rekisterinpitäjän on voitava osoittaa rekisteröidyn tekemä suostumus annetuksi	Rekisteröidyn antama suostumus, aikaleima

4.4	Rekisterinpitäjän on voitava tunnistaa, mistä rekisteröidyn henkilötiedot on saatu	Tiedonsaamisen tunnistetiedot, aikaleima Jos tietoja saadaan vain yhdestä lähteestä, riittää aikaleima (lähde kuvattu tietosuojaselosteessa)
4.6	Rekisterinpitäjän on tiedettävä, koska rekisteröity on saanut tiedon henkilötietojensa saamisesta	Rekisteröidyn kontaktoinnin aikaleima

Sovelluslogiikka

#	Otsikko	Käsittely
2.5	Rekisterinpitäjän on voitava osoittaa, mihin henkilötietojen käsittelytarkoitukseen liittyen rekisteröity on antanut suostumuksensa	Rekisteröidyn antaman suostumuksen aikaleiman raportointi, voidaan tarvita käsittelytarkoituksen laajentamisen yhteydessä
4.5	Rekisteröidylle on ilmoitettava kuukauden sisällä, jos hänen henkilötietojaan saadaan muualta kuin rekisteröidyltä itseltään	Toiselta rekisterinpitäjältä saatujen tietojen ja rekisteröidyn kontaktoinnin aikaleimavalvonta
4.27	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava käsitellä manuaalisesti automaattisesta päätöksenteosta estetyt henkilötiedot	Manuaalinen päätöksenteko, jos automaattinen on estetty Ilmoitus henkilötietojen käsittelijälle, jos manuaalisesti päätettävä asia odottaa
5.6	Rekisterinpitäjän tai henkilötietojen käsittelijän on voitava poistaa tai anonymisoida henkilötiedot säilytysajan päätyttyä	Poistoajo henkilötiedoille • fyysinen poisto • anonymisointi, kun säilytys aikasarjoja, tilastointia, arkistointia varten • pseudonymisointi, kun ei tarvetta enää tunnistaa rekisteröityä • tiedon maskaaminen, päällekirjoittaminen
5.11	Rekisterinpitäjän on huolehdittava henkilötietojen minimoinnista, jos henkilötietoja säilytetään erityisiä käsittelytarkoituksia varten	
7.1	Henkilötietojen käsittelijällä tulee olla oikeudet vain hänen tehtäviensä kannalta tarpeellisiin tietoihin	Sovelluksen toimintojen ml. käyttöliittymän jakaminen käyttäjäroolien mukaan
8.3	Rekisterinpitäjän on huolehdittava henkilötietojen käsittelyn lokittamisesta, jotta pystytään selvittämään loukatut rekisteröidyt ja henkilötiedot	Jokainen yksittäisen rekisteröidyn katselu, tallennus, muuttaminen ja poisto lokitetaan Jokainen poistoajossa poistettava tieto lokitetaan
8.7	Rekisterinpitäjän on pyrittävä määrittelemään ja löytämään tietovarantoihinsa tehtävät poikkeavat haut	?

Sovellusten testaus

#	Otsikko	Käsittely
8.1	Rekisterinpitäjän on riittävillä teknisillä toimilla estettävä ulkopuolelta tulevat hyökkäykset henkilötietoihin	Käyttöoikeuksien riittävä rajaavuus varmistettava Käyttöliittymäaukot tukittava, tietojen näkyvyyden rajaaminen varmistettava Rajapinnat testattava
8.2	Rekisterinpitäjän on testattava henkilötietoja käsittelevät järjestelmät sen varmistamiseksi, ettei tietoja vuoda vääriin käsiin	